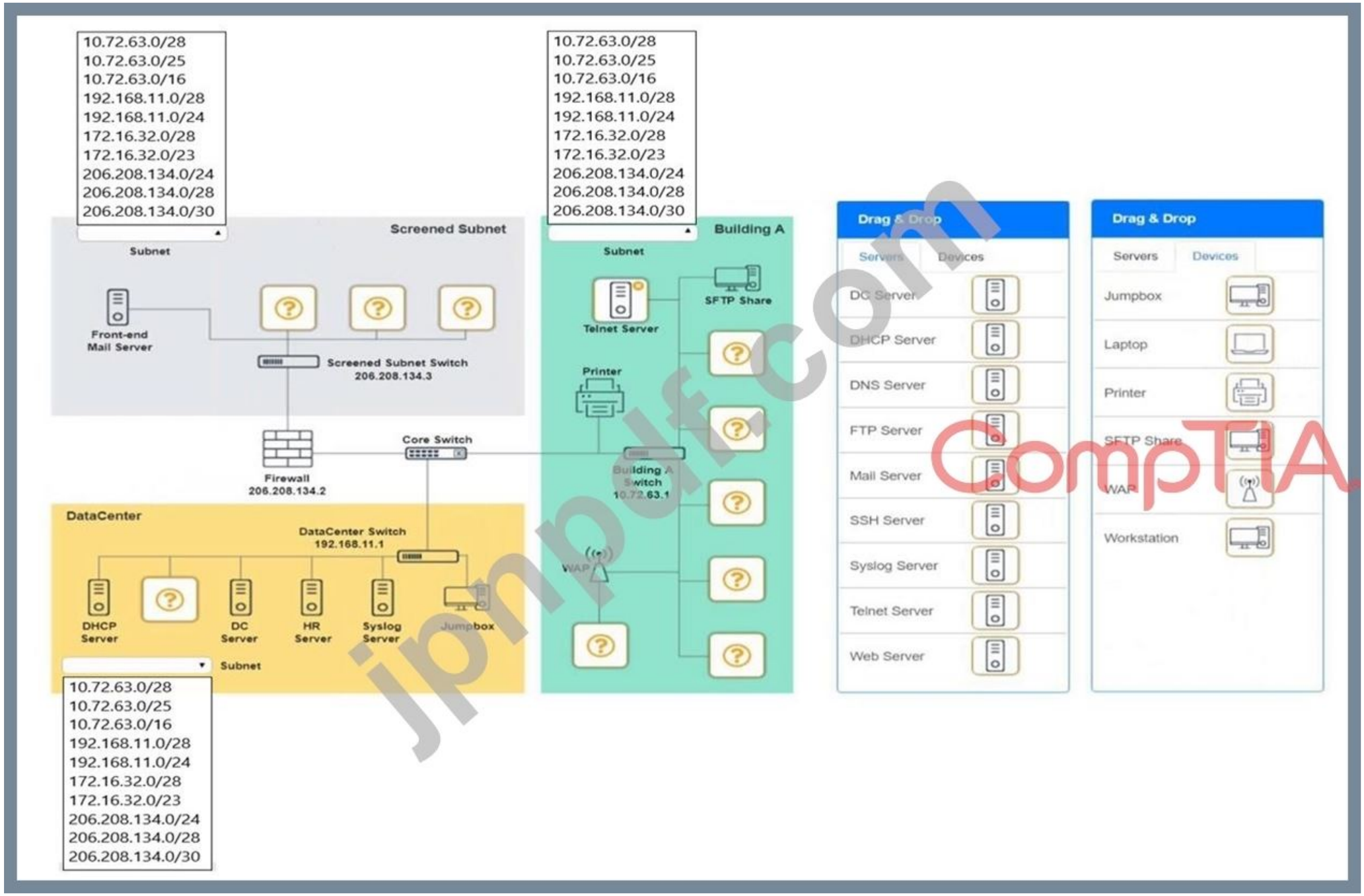
CompTIA.N10-009.v2024-12-16.q95

試験コード:	N10-009
試験名称:	CompTIA Network+ Certification Exam
認定資格:	CompTIA
無料問題数:	95
バージョン:	v2024-12-16
アクセス数:	3076
ページビュー数:	950
https://www.jpnpdf.com/CompTIA.N10-009.v2024-12-16.q95-mondaishu.html	

最新問題: **1**
ある組織では、すべてのネットワーク接続をユーザーまでさかのぼって追跡できるというセキュリティ要件があります。ネットワーク管理者は、ワイヤレス ネットワークに実装するソリューションを特定する必要があります。次のうち、最適なソリューションはどれですか。
A. エンタープライズ認証の実装
B. PSKの使用を要求する
C. ユーザー向けキャプティブポータルの設定
D. 有線と同等の保護の実施
Answer: A (メーッセージを残す**)**
エンタープライズ認証 (WPA2-Enterprise など) では、各ユーザーに固有の資格情報を使用し、通常は RADIUS などの認証サーバーと統合されます。これにより、ユーザー アクティビティの追跡とログ記録が可能になり、すべての接続を個々のユーザーにまでさかのぼることができます。PSK (事前共有キー) はユーザー間で共有され、個々の説明責任は提供されません。キャプティブ ポータルはユーザーを識別できますが、エンタープライズ認証よりも安全性が低く、Wired Equivalent Privacy (WEP) は時代遅れで、セキュリティ目的では推奨されません。

最新問題: **2**
ネットワーク セキュリティを確保するために、次の要件が満たされていることを確認する必要があります。
要件：
データセンター
ネットワークがサブネット化され、すべてのデバイスが適切に通信できるようになり、アドレス空間の使用量が最小限に抑えられることを確認します。IP アドレスとホスト名を正しく解決し、ポート 53 のトラフィックを処理する専用サーバーを用意します。建物 A ネットワークがサブネット化され、すべてのデバイスが適切に通信できるようになり、アドレス空間の使用量が最小限に抑えられることを確認します。5 人の追加のオフィス ユーザーをサポートするデバイスを用意します。モバイル ユーザーを追加します。Telnet サーバーをより安全なソリューションに置き換えます。スクリーン サブネット ネットワークがサブネット化され、すべてのデバイスが適切に通信できるようになり、アドレス空間の使用量が最小限に抑えられることを確認します。外部の 80/443 トラフィックを処理するサーバーを用意します。ポート 20/21 トラフィックを処理するサーバーを用意します。手順 オブジェクトを適切な場所にドラッグ アンド ドロップします。オブジェクトは複数回使用できます。また、すべてのプレースホルダーを埋める必要はありません。
使用可能なオブジェクトは、ドラッグ アンド ドロップ メニューの [サーバー] タブと [デバイス] タブの両方にあります。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。



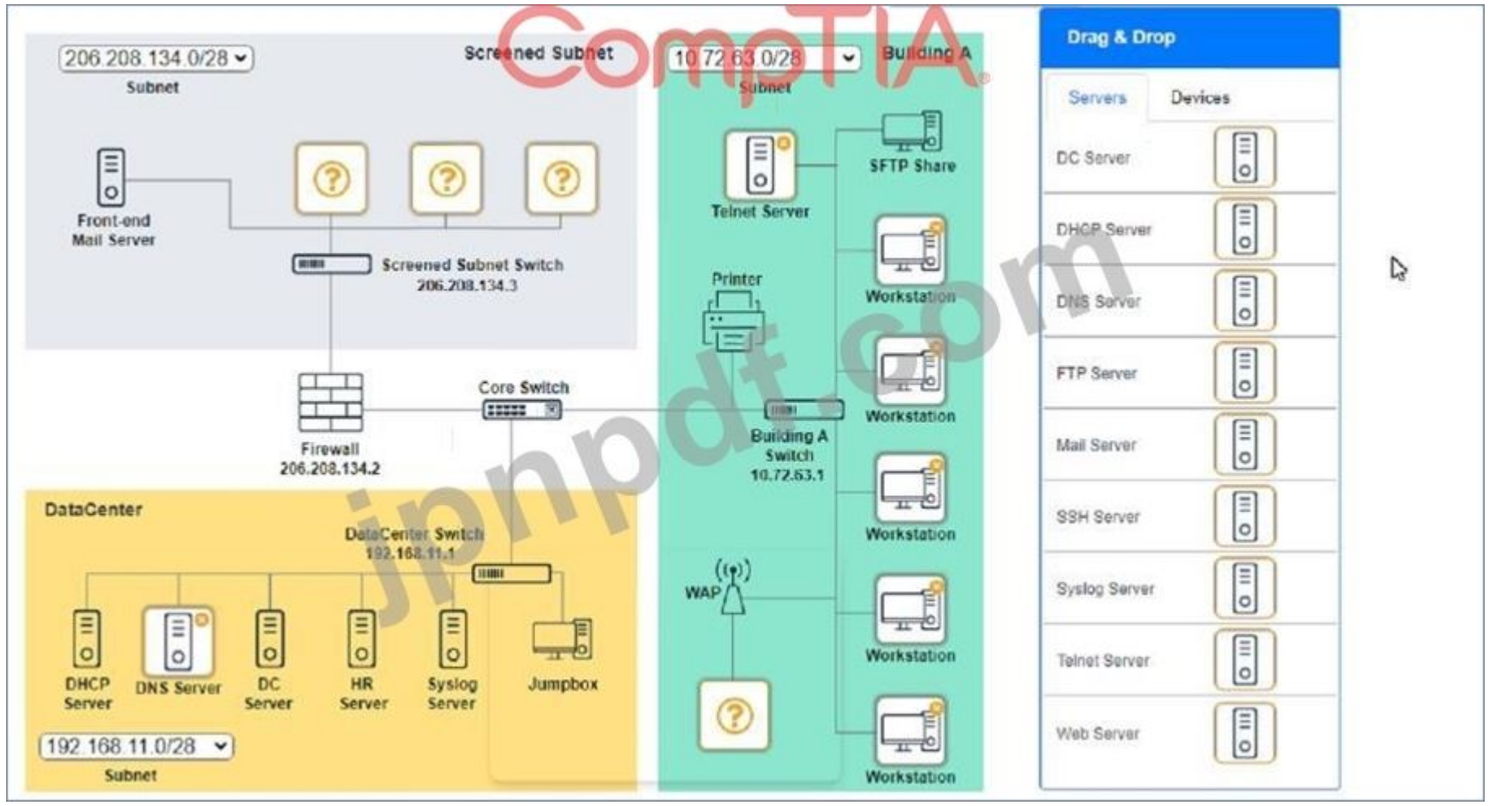
Answer:

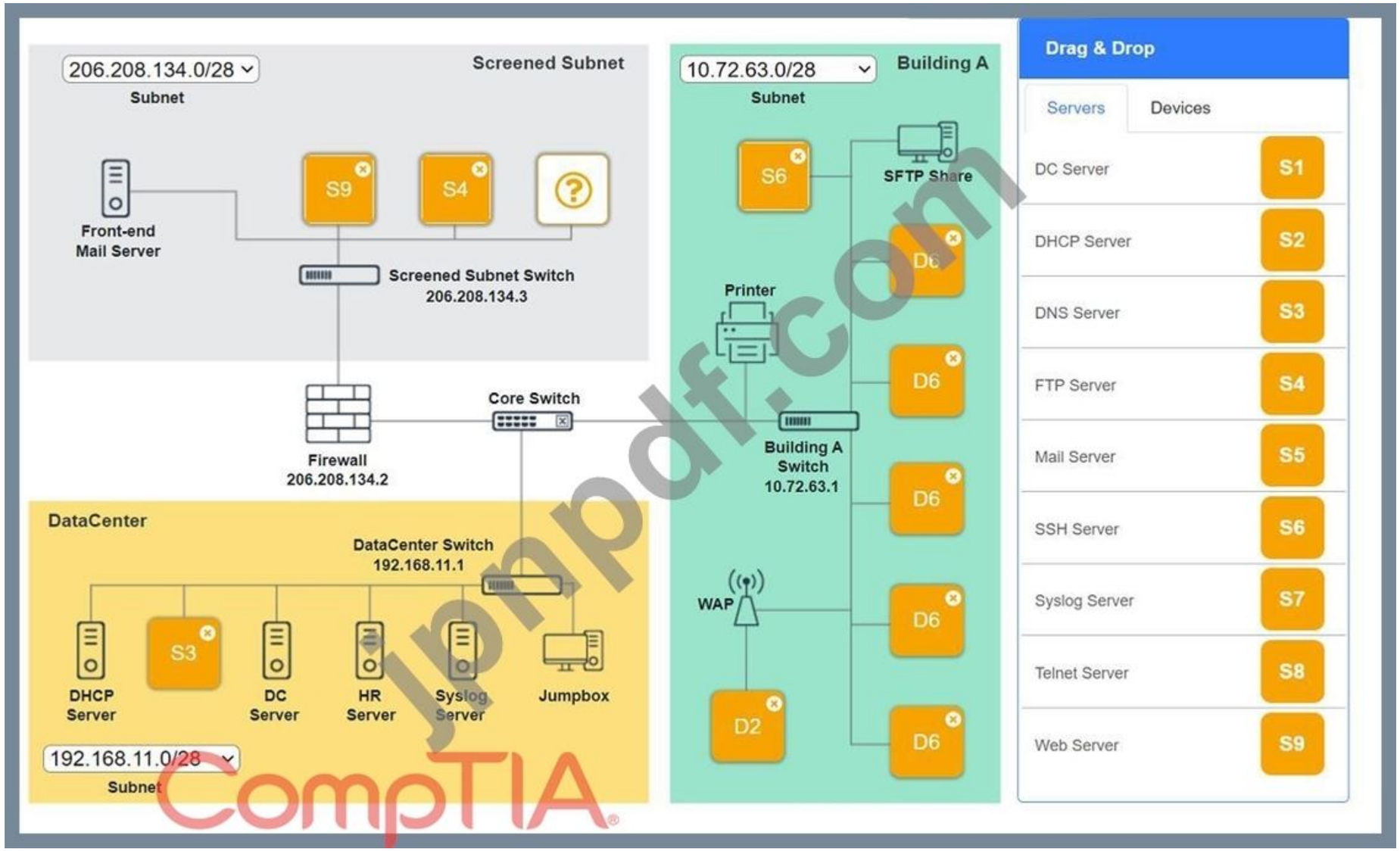
下記の説明を参照してください。

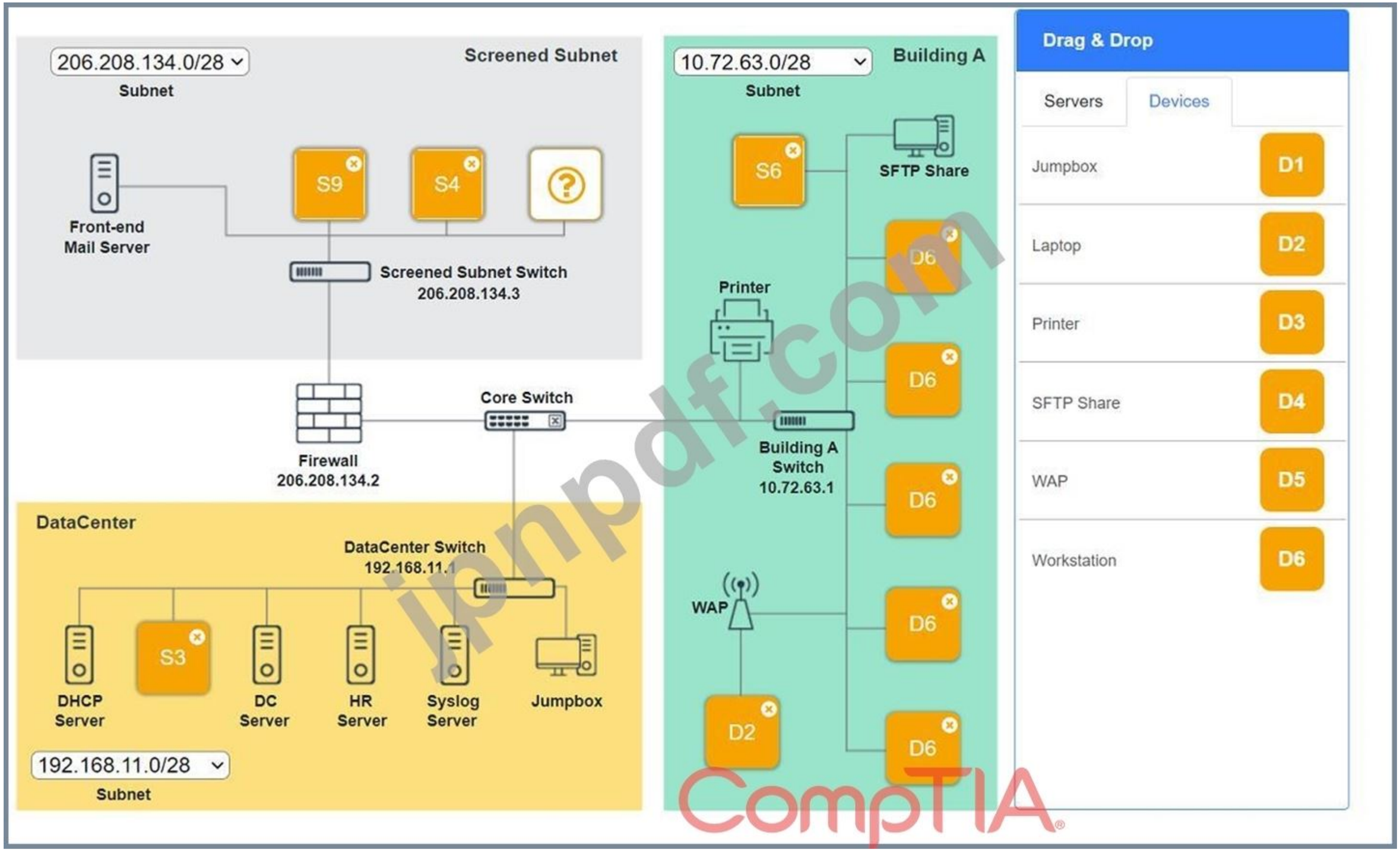
Explanation:

スクリーンサブネットデバイス - Webサーバー、FTPサーバー

建物 A のデバイス - 左上に SSH サーバー、右側に 5 台すべてのワークステーション、左下にラップトップ。データセンターのデバイス - DNS サーバー。


206.208.134.0/28
Subnet
Screened Subnet
Front-end
Mail Server
Screened Subnet Switch
206.208.134.3
Firewall
206.208.134.2
Core Switch
DataCenter
DataCenter Switch
192.168.11.1
DHCP
Server
DNS Server
DC
Server
HR
Server
Syslog
Server
Jumpbox
192.168.11.0/28
Subnet
10.72.63.0/28
Subnet
Building A
Telnet Server
SFTP Share
Printer
Workstation
Workstation
Building A
Switch
10.72.63.1
Workstation
WAP
Workstation
Workstation
Drag & Drop
Servers
Devices
DC Server
DHCP Server
DNS Server
FTP Server
Mail Server
SSH Server
Syslog Server
Telnet Server
Web Server


206.208.134.0/28
Subnet
Screened Subnet
Front-end
Mail Server
S9
S4
Screened Subnet Switch
206.208.134.3
Firewall
206.208.134.2
Core Switch
DataCenter
DataCenter Switch
192.168.11.1
S3
DHCP
Server
DC
Server
HR
Server
Syslog
Server
Jumpbox
192.168.11.0/28
Subnet
10.72.63.0/28
Subnet
Building A
S6
SFTP Share
D6
Printer
D6
Building A
Switch
10.72.63.1
D6
WAP
D6
D2
D6
Drag & Drop
Servers
Devices
DC Server
S1
DHCP Server
S2
DNS Server
S3
FTP Server
S4
Mail Server
S5
SSH Server
S6
Syslog Server
S7
Telnet Server
S8
Web Server
S9



最新問題: 3
次のどれがジャンボ フレームをサポートできますか?
A. アクセスポイント

B. ブリッジ
C. ハブ
D. スイッチ
Answer: (解答を表示する**)**
* ジャンボフレームの定義:
* ジャンボ フレームは、ペイロードが 1500 バイト以上 (通常は最大 9000 バイト) のイーサネット フレームです。ジャンボ フレームは、小さいフレームによって発生するオーバーヘッドを削減することで、ネットワーク パフォーマンスを向上させるために使用されます。
* スイッチがジャンボフレームをサポートする理由:
* スイッチは、データ パケットを管理するように設計されたネットワーク デバイスであり、ジャンボ フレームをサポートするように構成できます。この機能により、特に高性能ネットワークやデータ センターでスループットと効率が向上します。
* 他のデバイスとの非互換性:
* アクセス ポイント: 主にワイヤレス通信を処理し、通常はジャンボ フレームをサポートしません。
* ブリッジ:異なるネットワークセグメントを接続しますが、通常は標準のイーサネットフレームで動作します。
* サイズ。
* ハブ:デバイスを区別せずにすべてのポートにパケットを送信する、ジャンボフレームを処理できない単純なネットワークデバイス。
* 実用例:
* スイッチでジャンボ フレームを有効にすると、ストレージ エリア ネットワーク (SAN) や大規模な仮想化環境など、大量のデータ転送が頻繁に行われる環境で役立ちます。
参考文献:
* CompTIA Network+ コース教材とネットワーク ハードウェア ドキュメント。

最新問題: 4
ネットワーク技術者が、Web アプリケーションのパフォーマンス低下のトラブルシューティングを行っています。オフィスには、トラフィック負荷を共有する 2 つのインターネット リンクがあります。技術者は、Web アプリケーションに使用されているリンクを判断するために、次のどのツールを使用する必要がありますか。
A. ネットスタット
B. nslookup
C. ピン
D. トレース
Answer: D (メーッセージを残す**)**
Tracert を理解する:
Traceroute ツール: tracert (Windows) または traceroute (Linux) は、パケットが送信元から送信先までたどるパスを追跡するために使用されるネットワーク診断ツールです。パケットが通過するすべての中間ルーターを一覧表示します。
トラフィック パスの決定:
パス識別: Web アプリケーションの宛先 IP アドレスに対して tracert を実行することで、技術者はトラフィックがどのルートをたどっているかを特定し、どのインターネット リンクが使用されているかを判断できます。
負荷分散の洞察: オフィスがインターネット リンクに負荷分散を使用している場合、tracert を使用すると、現在どのリンクが Web アプリケーションのトラフィックを処理しているかを確認できます。
他のツールとの比較:
netstat: ネットワーク接続、ルーティング テーブル、インターフェイス統計などを表示しますが、パケットのパスは追跡しません。
nslookup: パケット ルートのトレースではなく、ドメイン名または IP アドレスのマッピングを取得するために DNS を照会するために使用されます。
ping: 接続性をテストし、往復時間を測定しますが、パス情報は提供しません。
実装：

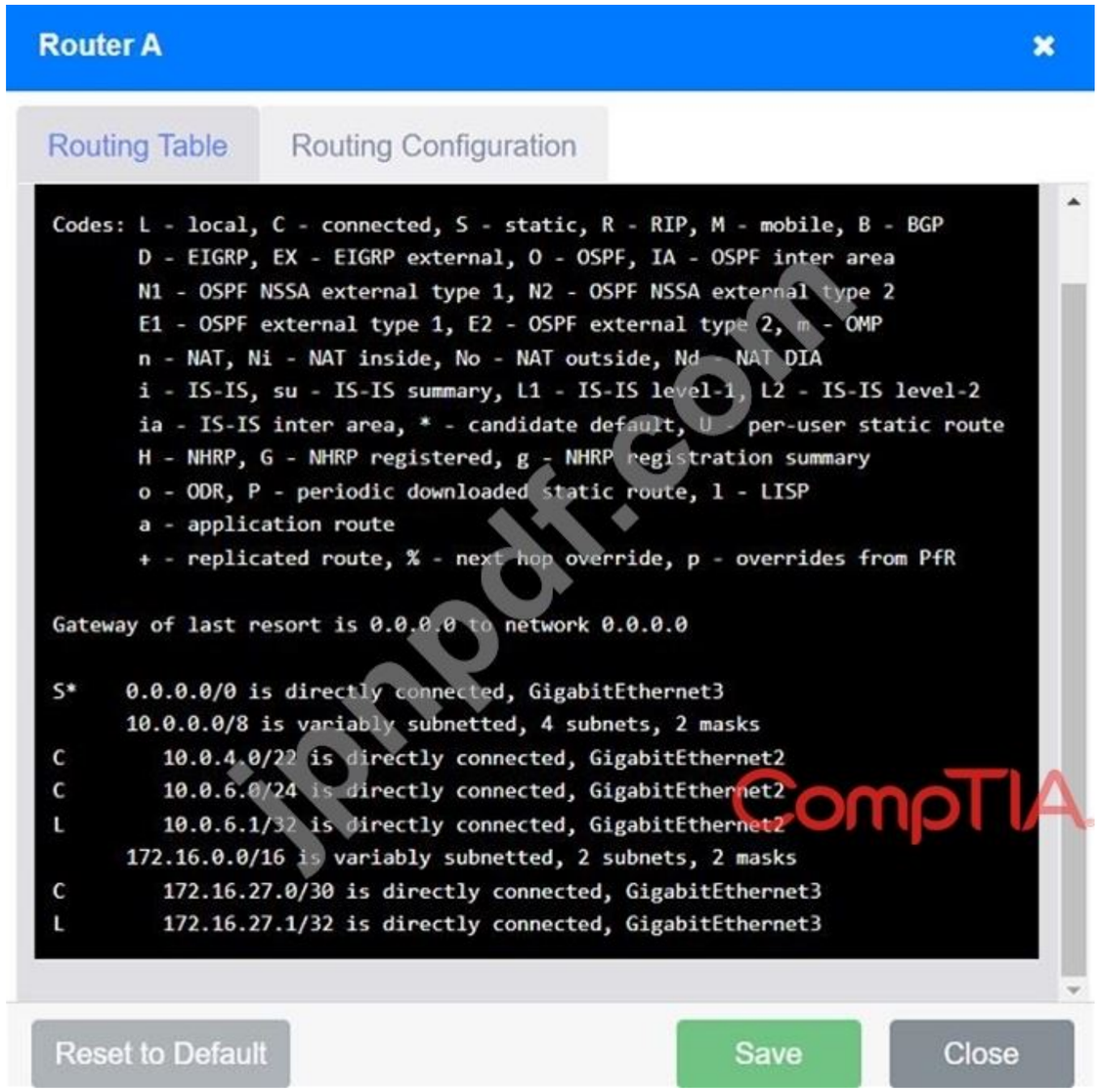
コマンドプロンプトまたはターミナルを開きます。
ルートをトレースするには、tracert [宛先 IP] を実行します。
出力を分析して、使用されているパスとリンクを特定します。
参照：
ネットワークのトラブルシューティングと診断ツールに関する CompTIA Network+ 学習教材。

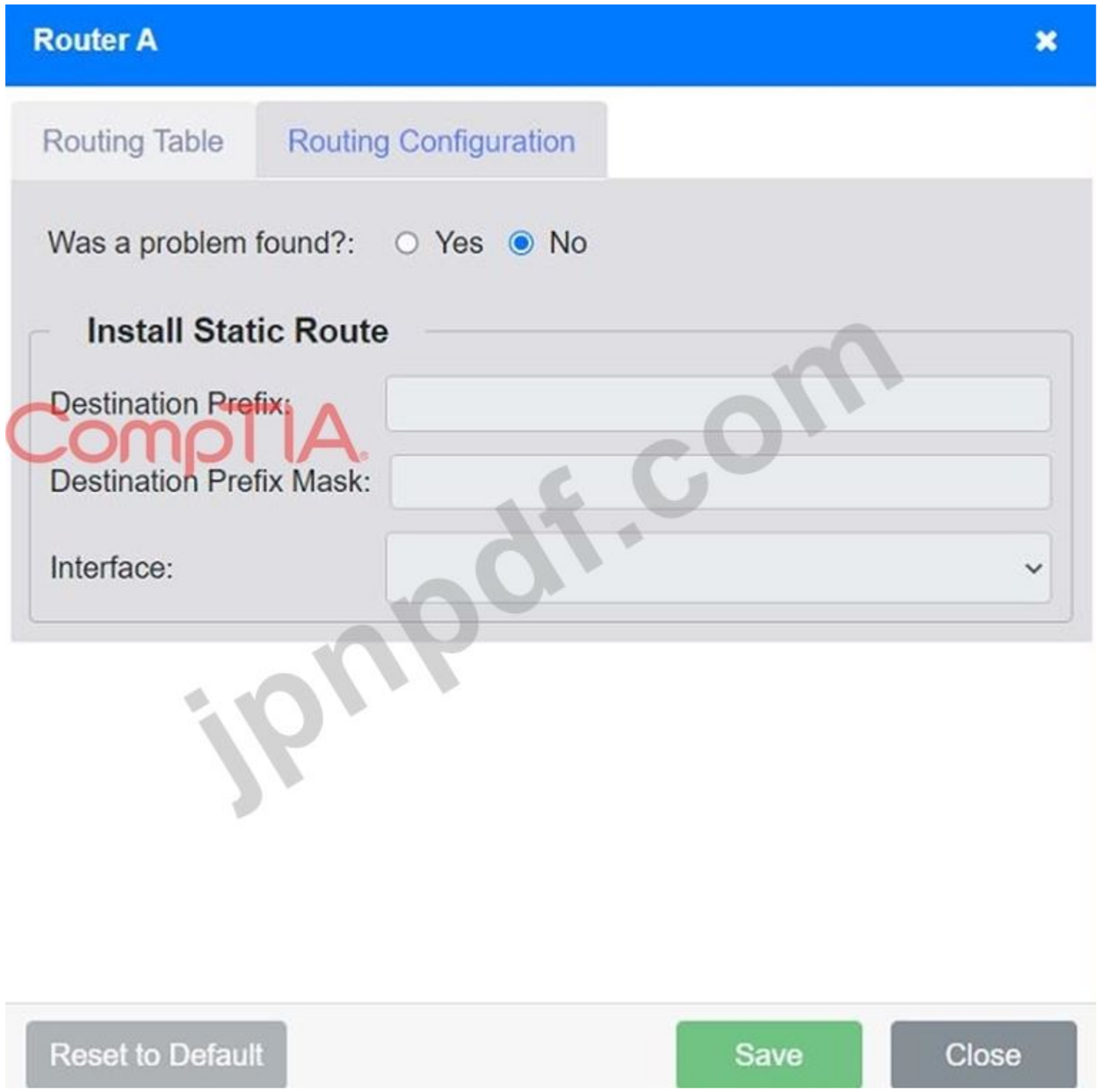
最新問題**: 5**
ネットワーク管理者は、ルーターのインターフェイスを 10.0.0.95 255.255.255.240 に設定しました。管理者は、ルーターが IP 10.0.0.81/28 の Web サーバーにパケットをルーティングしていないことを発見しました。次のどれが最適な説明ですか?
A. Web サーバーは別のサブネットにあります。
B. ルーターのインターフェースはブロードキャスト アドレスです。
C. IP アドレス空間はクラス A ネットワークです。
D. サブネットはプライベート アドレス空間内にあります。
Answer: B (メーッセージを残す**)**
サブネット化の理解:
サブネット マスク 255.255.255.240 (または /28) は、各サブネットに 16 個の IP アドレス (使用可能なアドレスが 14 個、ネットワーク アドレスが 1 個、ブロードキャスト アドレスが 1 個) があることを示します。
サブネット範囲の計算:
サブネットの計算: /28 サブネット マスクを持つ IP アドレス 10.0.0.95 の場合:
ネットワークアドレス: 10.0.0.80
使用可能な IP 範囲: 10.0.0.81 〜 10.0.0.94
ブロードキャストアドレス: 10.0.0.95
ルーターのインターフェース構成:
ブロードキャスト アドレスの問題: IP アドレス 10.0.0.95 は、サブネット 10.0.0.80/28 のブロードキャスト アドレスです。ブロードキャスト アドレスを使用してルーター インターフェイスを構成すると、有効なホスト アドレスではないため、ルーティングの問題が発生します。
他のオプションとの比較:
Web サーバーは別のサブネットにあります: Web サーバー (10.0.0.81) は同じサブネット範囲 (10.0.0.80/28) 内にあります。
IP アドレス空間はクラス A ネットワークです。10.0.0.0 はクラス A ネットワークですが、ブロードキャスト アドレスによって発生するルーティングの問題は説明されません。
サブネットはプライベート アドレス空間内にあります: プライベート アドレス空間の指定 (RFC 1918) は、ブロードキャスト アドレス構成に関連するルーティングの問題には影響しません。
解決：
使用可能な範囲内の有効なホスト IP アドレス (10.0.0.94 など) を使用して、ルーターのインターフェイスを再設定します。
参照：
サブネットと IP アドレス構成に関する CompTIA Network+ 学習教材。

最新問題**: 6**
次のルーティング プロトコルのうち、自律システム番号を使用するものはどれですか?
A. イスイス
B. EIGRP
C. OSPF
D. BGP

Answer: (解答を表示する**)**
BGP (Border Gateway Protocol) は、その動作に自律システム (AS) 番号を使用します。AS は、インターネットに共通のルーティング ポリシーを提示する単一の組織の管理下にある IP ネットワークとルーターの集合です。BGP は、インターネット上の異なる AS 間でルーティング情報を交換するために使用されるため、リストされているオプションの中で AS 番号を使用する唯一のプロトコルです。
参考: CompTIA Network+ 学習教材および RFC 4271。

最新問題**: 7**
シミュレーション
ユーザーは、ファイル サーバー 2 にある部門共有上のファイルにアクセスできません。
ネットワーク管理者は、ワークステーション A とファイル サーバー 2 をホストするネットワーク間のルーティングを検証する役割を担っています。
説明書
各ルータをクリックして出力を確認し、問題を特定し、適切なソリューションを構成します。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。




Router A
Routing Table
Routing Configuration
Was a problem found?:
Yes
No
Install Static Route
Destination Prefix:
Destination Prefix Mask:
Interface:
Reset to Default
Save
Close

Router C

Routing Table | Routing Configuration

```
Router-C# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.0.0.0/22 [1/0] via GigabitEthernet1
S        10.0.4.0/22 [1/0] via GigabitEthernet2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.0/30 is directly connected, GigabitEthernet2
L        172.16.27.2/32 is directly connected, GigabitEthernet2
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.6/32 is directly connected, GigabitEthernet1
```

Reset to Default | Save | Close


Router B
CompTIA
Routing Table
Routing Configuration
Router-B# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S* 0.0.0.0/0 is directly connected, GigabitEthernet1
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.0.0/22 is directly connected, GigabitEthernet3
L 10.0.0.1/32 is directly connected, GigabitEthernet3
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.27.4/30 is directly connected, GigabitEthernet1
L 172.16.27.5/32 is directly connected, GigabitEthernet1
Reset to Default
Save
Close

Answer:
説明の解決策を参照
Explanation:
ワークステーション A とファイル サーバー 2 をホストするネットワーク間のルーティングを検証するには、次の手順に従います。
ステップバイステップのソリューション
ルーティング テーブルを確認する:
ルータ A、ルータ B、ルータ C のルーティング テーブルをチェックして、不足しているルートを特定します。
欠落しているルートを特定する:
各ルータに、ワークステーション A とファイル サーバー 2 が配置されているネットワークへのルートがあることを確認します。
静的ルートを追加します。
ルートが見つからない場合は、正しいインターフェースを介して関連する宛先ネットワークへの静的ルートを追加します。
詳細な分析と構成
ルーターA:
ルーティングテーブル:
最後のゲートウェイは 0.0.0.0 からネットワーク 0.0.0.0 です
S* 0.0.0.0/0は直接接続され、GigabitEthernet3
10.0.0.0/8 は可変サブネット化されており、4 つのサブネットと 2 つのマスクがあります。
C 10.0.4.0/22は直接接続され、GigabitEthernet2
C 10.0.6.0/24は直接接続され、GigabitEthernet2

L 10.0.6.1/32は直接接続され、GigabitEthernet2
172.16.0.0/16 は可変サブネット化されており、サブネットは 2 つ、マスクは 2 つ
C 172.16.27.0/30は直接接続され、GigabitEthernet3
L 172.16.27.1/32は直接接続され、GigabitEthernet3
ルーターB:
ルーティングテーブル:
最後のゲートウェイは 0.0.0.0 からネットワーク 0.0.0.0 です
S* 0.0.0.0/0は直接接続され、GigabitEthernet1
10.0.0.0/8 は可変サブネット化されており、4 つのサブネットと 2 つのマスクがあります。
C 10.0.0.0/22は直接接続され、GigabitEthernet1
L 10.0.0.1/32は直接接続され、GigabitEthernet1
172.16.0.0/16 は可変サブネット化されており、サブネットは 2 つ、マスクは 2 つ
C 172.16.27.4/30は直接接続され、GigabitEthernet1
L 172.16.27.5/32は直接接続され、GigabitEthernet1
ルーターC:
ルーティングテーブル:
10.0.0.0/8 は可変サブネット化されており、4 つのサブネットと 2 つのマスクがあります。
S 10.0.0.0/22 [1/0] GigabitEthernet1経由
S 10.0.4.0/22 [1/0] GigabitEthernet2経由
172.16.0.0/16 は可変サブネット化されており、サブネットは 2 つ、マスクは 2 つ
C 172.16.27.0/30は直接接続され、GigabitEthernet2
L 172.16.27.2/32は直接接続され、GigabitEthernet2
C 172.16.27.4/30は直接接続され、GigabitEthernet1
L 172.16.27.6/32は直接接続され、GigabitEthernet1
設定手順:
ルーターA:
172.16.27.1 経由で 10.0.0.0/22 への静的ルートをインストールします (ルータ C の IP が 172.16.27.1 であると仮定)。
宛先プレフィックス: 10.0.0.0
宛先プレフィックスマスク: 255.255.252.0
インターフェース: GigabitEthernet3
ルーターB:
172.16.27.5 経由で 10.0.4.0/22 への静的ルートをインストールします (ルータ C の IP が 172.16.27.5 であると仮定)。
宛先プレフィックス: 10.0.4.0
宛先プレフィックスマスク: 255.255.252.0
インターフェース: GigabitEthernet1
ルーターC:
172.16.27.2 経由で 10.0.6.0/24 への静的ルートをインストールします (ルータ A の IP が 172.16.27.2 であると仮定)。
宛先プレフィックス: 10.0.6.0
宛先プレフィックスマスク: 255.255.255.0
インターフェース: GigabitEthernet2

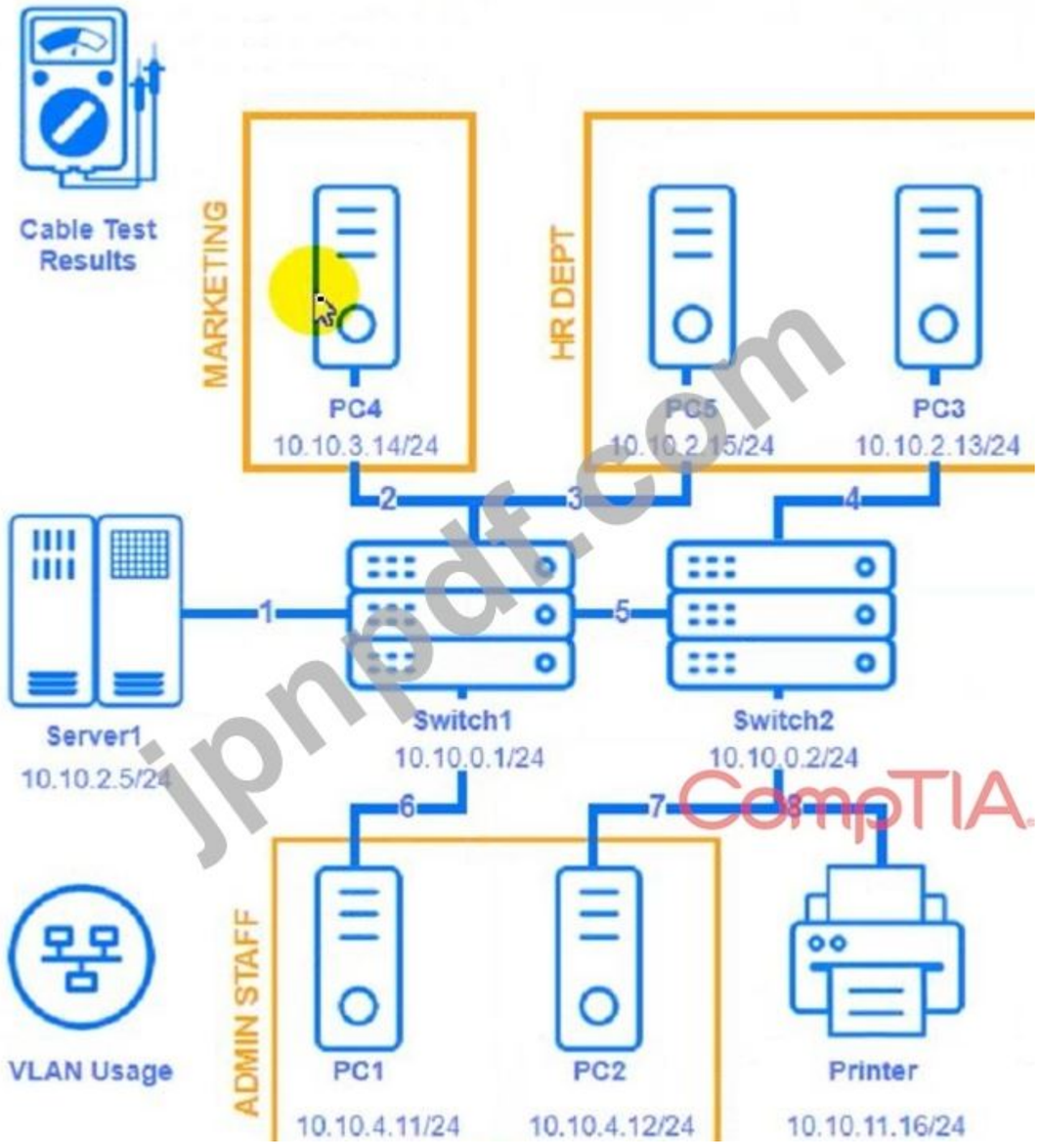
172.16.27.1 経由で 10.0.0.0/22 への静的ルートをインストールします (ルータ B の IP が 172.16.27.1 であると仮定)。
宛先プレフィックス: 10.0.0.0
宛先プレフィックスマスク: 255.255.252.0
インターフェース: GigabitEthernet1
静的ルートの概要:
ルーターA:
IPルート10.0.0.0 255.255.252.0 ギガビットイーサネット3
ルーターB:
IPルート10.0.4.0 255.255.252.0 ギガビットイーサネット1
ルーターC:
IPルート10.0.6.0 255.255.255.0 ギガビットイーサネット2
IPルート 10.0.0.0 255.255.252.0 ギガビットイーサネット1
これらの構成により、各ルータがワークステーション A とファイル サーバー 2 に到達するための正しいパスを認識するようになり、接続の問題が解決されます。

最新問題**: 8**
次のどれがジャンボ フレームをサポートできますか?
A. アクセスポイント
B. ブリッジ
C. ハブ
D. スイッチ
Answer: D (メーッセージを残す**)**
* ジャンボフレームの定義:
* ジャンボ フレームは、ペイロードが 1500 バイト以上 (通常は最大 9000 バイト) のイーサネット フレームです。ジャンボ フレームは、小さいフレームによって発生するオーバーヘッドを削減することで、ネットワーク パフォーマンスを向上させるために使用されます。
* スイッチがジャンボフレームをサポートする理由:
* スイッチは、データ パケットを管理するように設計されたネットワーク デバイスであり、ジャンボ フレームをサポートするように構成できます。この機能により、特に高性能ネットワークやデータ センターでスループットと効率が向上します。
* 他のデバイスとの非互換性:
* アクセス ポイント: 主にワイヤレス通信を処理し、通常はジャンボ フレームをサポートしません。
* ブリッジ: 異なるネットワーク セグメントを接続しますが、通常は標準のイーサネット フレーム サイズで動作します。
* ハブ: デバイスを区別せずにすべてのポートにパケットを送信する、ジャンボ フレームを処理できない単純なネットワーク デバイス。
* 実用例:
* スイッチでジャンボ フレームを有効にすると、ストレージ エリア ネットワーク (SAN) や大規模な仮想化環境など、大量のデータ転送が頻繁に行われる環境で役立ちます。
参考文献:
* CompTIA Network+ コース教材とネットワーク ハードウェア ドキュメント。

最新問題**: 9**
ネットワーク管理者は、有線デバイスと無線デバイスの両方にアクセスするときに、ユーザーがポートベースの認証フレームワークを使用して企業ネットワークに認証できるようにしたいと考えています。このタスクを実行するのに最適なセキュリティ機能はどれですか。
A. 802.1X

B. アクセス制御リスト
C. ポートセキュリティ
D. MACフィルタリング
Answer: (解答を表示する**)**
802.1X は、LAN または WLAN に接続するデバイスに認証メカニズムを提供するポートベースのネットワーク アクセス制御 (PNAC) プロトコルです。これは、有線または無線の手段で接続する場合でも、認証されたデバイスのみがネットワークにアクセスできるようにする、安全なネットワーク アクセスのために広く使用されています。
802.1X は、RADIUS などの認証サーバーと連携して、接続しようとしているデバイスの資格情報を検証します。参考資料:CompTIA Network+ 学習教材。

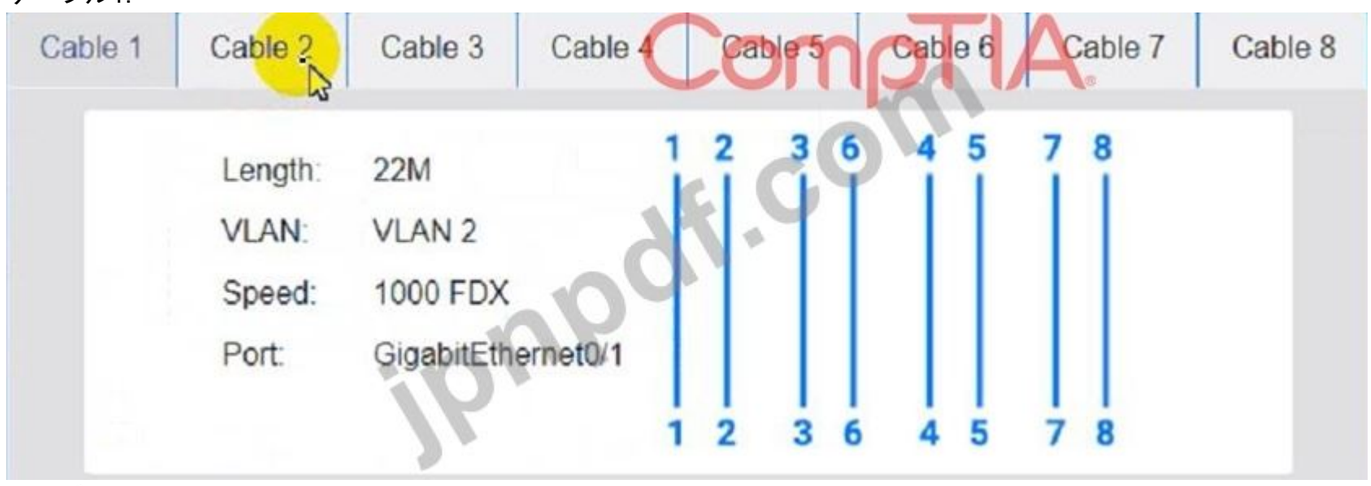
最新問題**: 10**
シミュレーション
ネットワーク技術者は、顧客の SOHO ネットワークに関するいくつかの問題を解決する必要があります。
顧客は、一部のデバイスがネットワークに接続されていないが、他のデバイスは意図したとおりに動作しているようだと報告しています。
説明書
各デバイスとケーブルをクリックして、すべてのネットワーク コンポーネントのトラブルシューティングを行い、ケーブル テストの結果を確認します。
問題のあるコンポーネントを特定して適切なコンポーネントを診断し、各問題を修正するための解決策を提案します。


Cable Test Results
MARKETING
HR DEPT
PC4
10.10.3.14/24
PC5
10.10.2.15/24
PC3
10.10.2.13/24
2
3
4
1
5
Server1
10.10.2.5/24
Switch1
10.10.0.1/24
Switch2
10.10.0.2/24
6
7
8
VLAN Usage
ADMIN STAFF
PC1
10.10.4.11/24
PC2
10.10.4.12/24
Printer
10.10.11.16/24

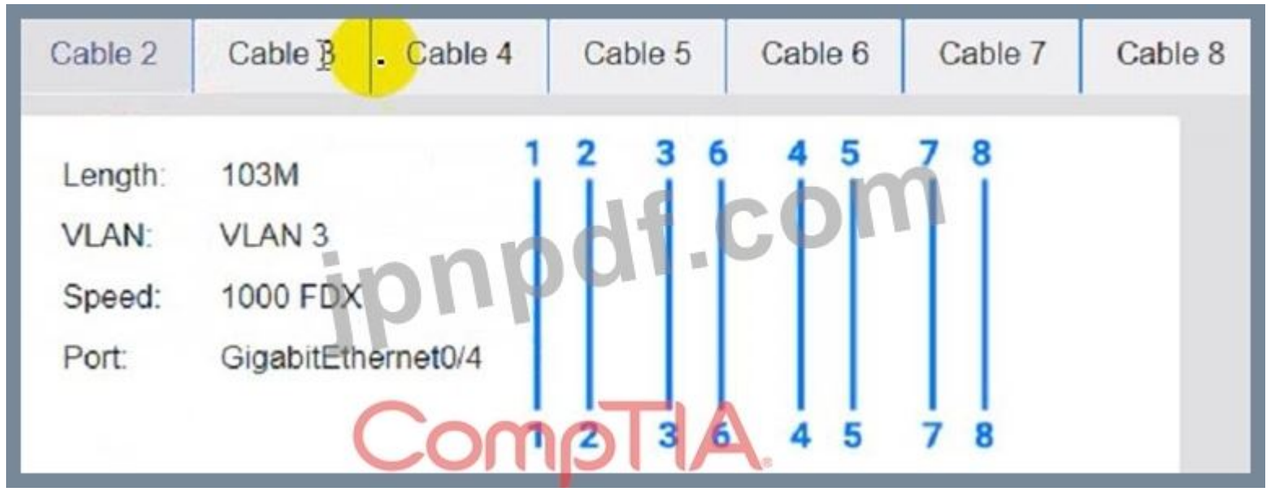

PC1 - ADMIN STAFF
C:\>
jnpdf.com
CompTIA
PC3 - HR DEPT
CompTIA
C:\>
jnpdf.com

ケーブルテスト結果:

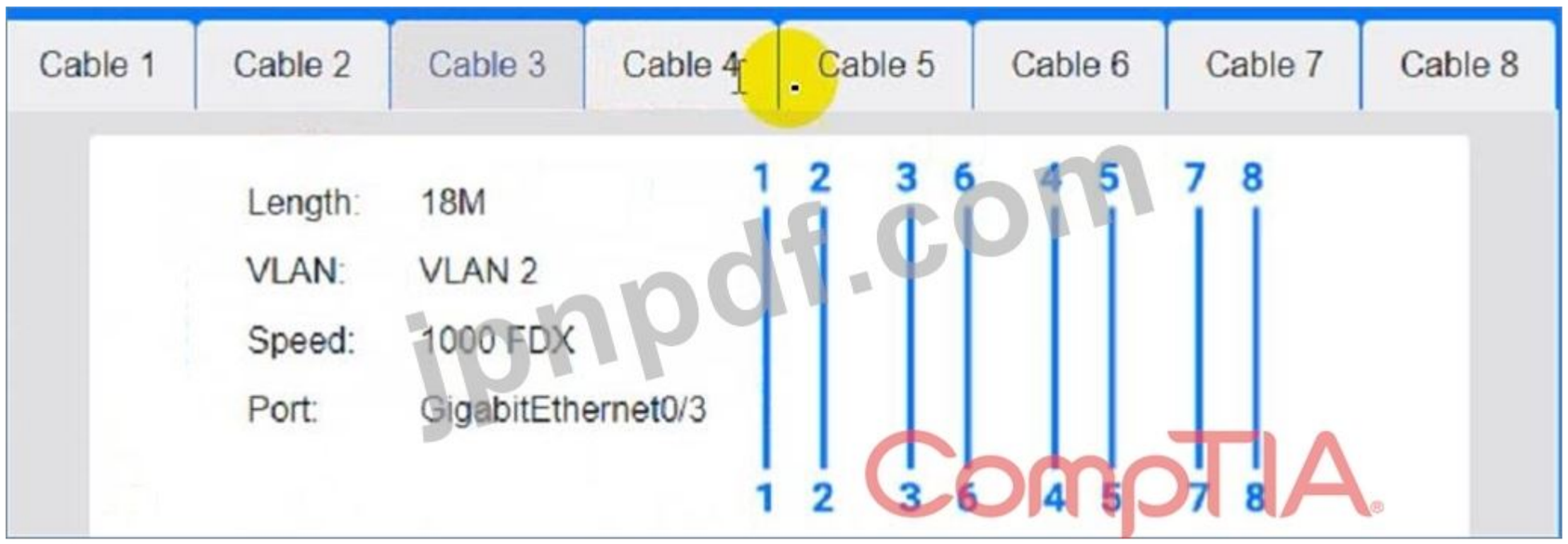
ケーブル1:



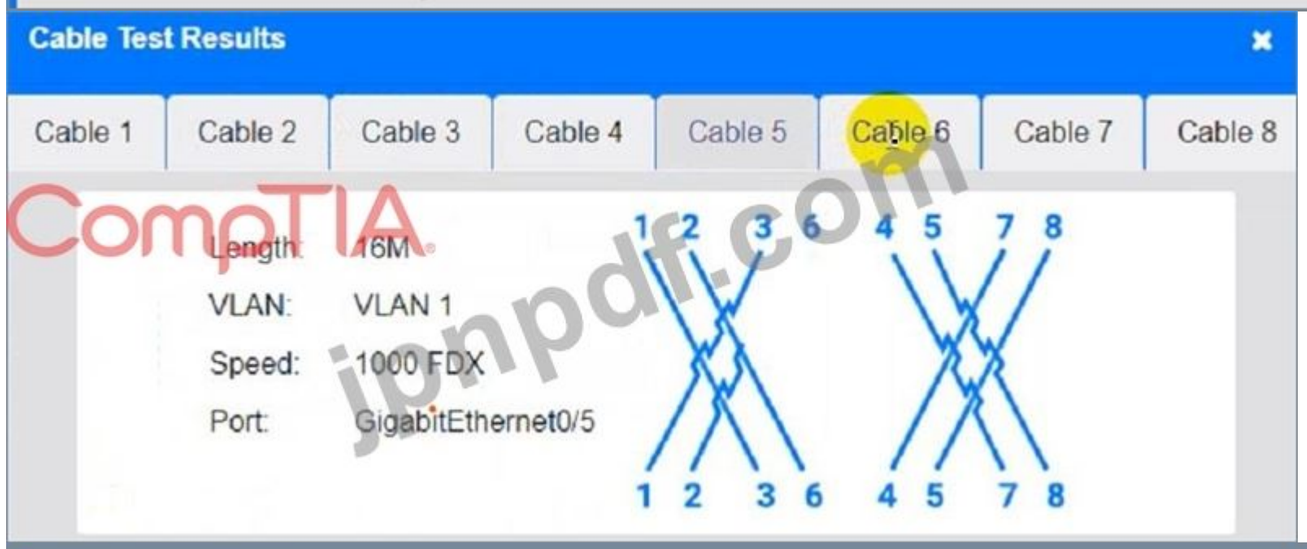
ケーブル2:

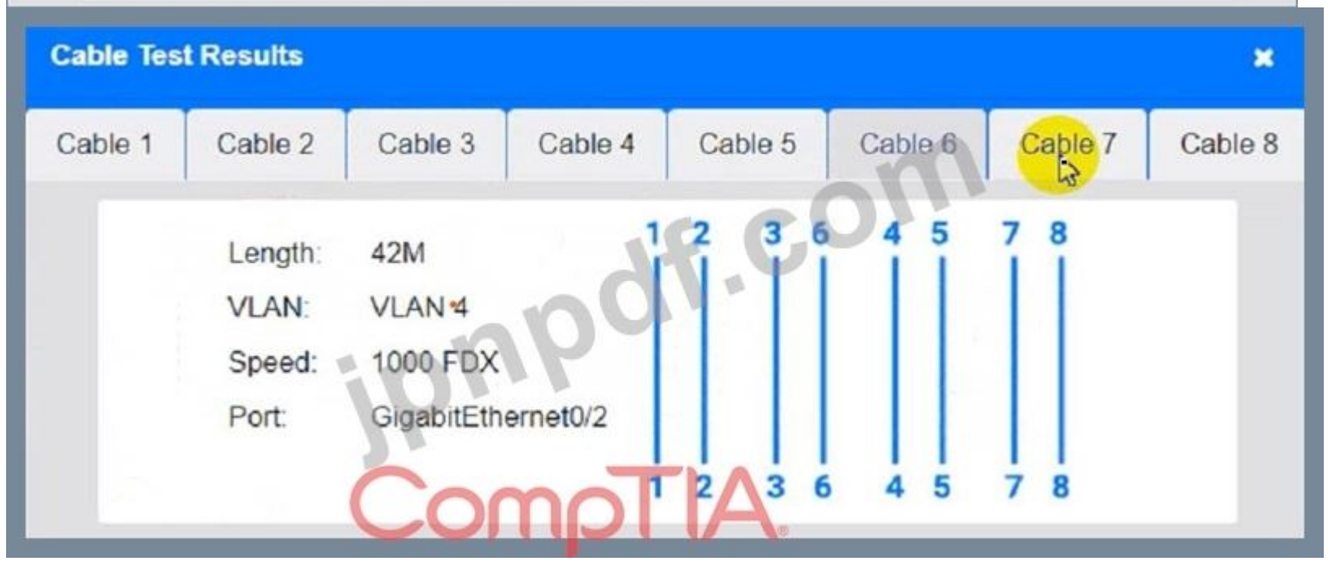

Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 103M
VLAN: VLAN 3
Speed: 1000 FDX
Port: GigabitEthernet0/4
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

ケーブル3:


Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 18M
VLAN: VLAN 2
Speed: 1000 FDX
Port: GigabitEthernet0/3
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

ケーブル4:

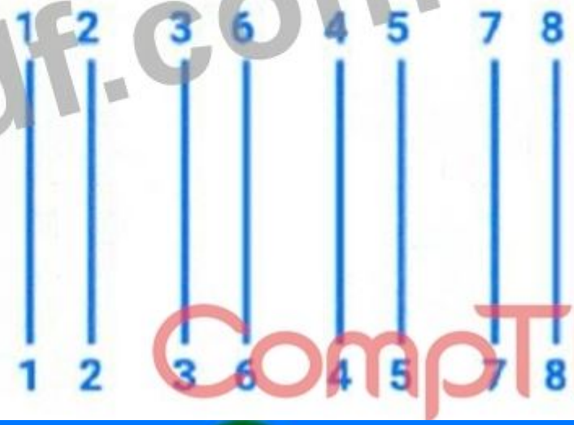




Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

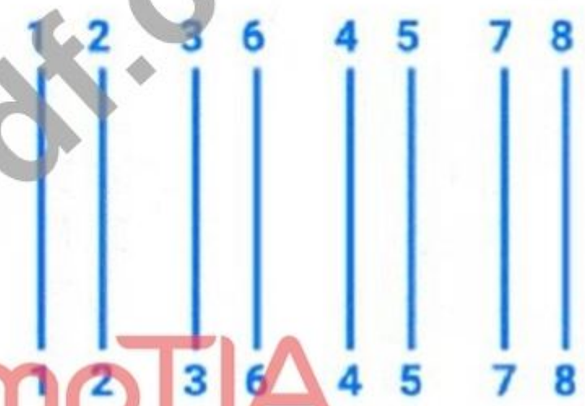
Length: 12M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/1



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

Length: 90M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/3



Printer

HP Network Configuration Page

Model: HP Officejet Pro 8610

General Information

Network Status	Ready
Active Connection Type	Wired
URL(s) for Embedded Web Server	http://HP4D30EC, http://192.168.2.9
Firmware Revision	FDP1CN1347AR
Hostname	HP4D30EC
Serial Number	CN3AO1KG42
Internet	Not Connected

802.3 Wired

Hardware Address (MAC)	9c:b6:54:4d:30:ec

Answer:

このシミュレーションの詳細については説明を参照してください

Explanation:

(注: Ips は各シミュレーション タスクで変更されるため、理解を深めるために回答例を示します) すべてのネットワーク コンポーネントのトラブルシューティングを行い、ケーブル テストの結果を確認するには、次の手順に従います。

各デバイスとケーブルをクリックすると、情報ウィンドウが開きます。

情報を確認し、ネットワーク接続やパフォーマンスに影響する可能性のある問題やエラーを特定します。

問題のあるコンポーネントを特定して適切なコンポーネントを診断し、各問題を修正するための解決策を提案します。

提供されているドロップダウン メニューを使用して修復フォームに入力します。

PC1 の修復フォームに記入する方法の例を次に示します。

問題のあるコンポーネントは PC1 です。

問題はIPアドレスが正しくないことです。

解決策は、IP アドレスを 192.168.1.10 に変更することです。
同じ手順を使用して、他のコンポーネントの修復フォームに入力できます。
各デバイスにコマンドを入力するには、次の手順に従います。
デバイスをクリックすると、ターミナル ウィンドウが開きます。
ipconfig /all コマンドを入力すると、デバイスの IP アドレス、サブネット マスク、デフォルト ゲートウェイ、DNS サーバーなどの IP 構成が表示されます。
エコー パケットを送受信して、ネットワーク上の別のデバイスへの接続性と到達可能性をテストするには、コマンド ping <IP アドレス> を入力します。<IP アドレス> を、コア スイッチ 1 の場合は 192.168.1.1 など、宛先デバイスの IP アドレスに置き換えます。
コマンド tracert <IP アドレス> を入力してルートをトレースし、TTL 値を増やしながらパケットを送受信して、デバイスからネットワーク上の別のデバイスへのパケットの遅延を測定します。<IP アドレス> を、コア スイッチ 1 の場合は 192.168.1.1 など、宛先デバイスの IP アドレスに置き換えます。
PC1 でコマンドを入力する方法の例を次に示します。
PC1 をクリックしてターミナル ウィンドウを開きます。
ipconfig /all コマンドを入力して、PC1 の IP 構成を表示します。PC1 の IP アドレスが 192.168.2.10 と正しくなく、VLAN 1 ではなく VLAN 2 に属していることがわかります。
コア スイッチ 1 への接続をテストするには、コマンド ping 192.168.1.1 を入力します。PC1 とコア スイッチ 1 は異なるサブネット上にあるため、PC1 はコア スイッチ 1 に ping できないことがわかります。
コマンド tracert 192.168.1.1 を入力して、コア スイッチ 1 へのルートをトレースします。PC1 とコア スイッチ 1 の間にルートがないため、PC1 がコア スイッチ 1 に到達できないことがわかります。
同じ手順を使用して、PC3、PC4、PC5、サーバー 1 などの他のデバイスにコマンドを入力できます。

最新問題: 11
提供された URL が正しい IP アドレスに解決されないため、ユーザーは Web サイトに移動できません。
他のユーザーは問題なく目的の Web サイトに移動できます。この問題の原因として最も可能性が高いのは次のどれですか?
A. ホストファイル
B. 自己署名証明書
C. ネームサーバーレコード
D. IP ヘルパー ANS
Answer: A (メーッセージを残す**)**
* Hosts ファイルの役割:
* hosts ファイルは、ホスト名を IP アドレスにマッピングするコンピュータ上のローカル ファイルです。ホスト名を IP アドレスに静的にマッピングすることで、DNS 解決をオーバーライドするために使用できます。
* Hosts ファイルに関する一般的な問題:
* ホスト ファイル内のホスト名に誤った IP アドレスがマップされている場合、コンピューターがホスト名を誤った IP アドレスに解決する可能性があります。これにより、特定の Web サイトでナビゲーションの問題が発生する可能性がありますが、DNS に依存している他のユーザーには同じ問題はありません。
* 他の選択肢の可能性が低い理由:
* 自己署名証明書: SSL/TLS に関連し、ナビゲーションの失敗ではなく、セキュリティ警告が発生します。
* ネームサーバーレコード: 1 人のユーザーだけでなく、すべてのユーザーに影響します。
* IP ヘルパー:DHCP 要求を転送するために使用され、DNS 解決の問題とは無関係です。
* トラブルシューティングの手順:
* 影響を受けるユーザーのコンピューター上の hosts ファイルを確認します (Windows の場合は C:\Windows\System32\drivers\etc\host、Unix/Linux の場合は /etc/host)。
* 問題のあるホスト名を誤った IP アドレスにマッピングするエントリを探し、修正または削除します。
参考文献:

* CompTIA Network+ の学習教材とシステム管理ドキュメント。

最新問題**: 12**
ネットワーク管理者のデバイスは、企業本社内で深刻な Wi-Fi 干渉を受けており、デバイスが頻繁にネットワークから切断される状態になっています。この問題の原因として最も可能性が高いのは次のどれですか。
A. 無線反射が多すぎる
B. 無線吸収が多すぎる
C. 無線リピーターが多すぎます
D. クライアント接続が多すぎます
Answer: (解答を表示する**)**
企業本社内で深刻な Wi-Fi 干渉が発生し、デバイスが頻繁にネットワークから切断される場合は、無線反射が多すぎることが原因である可能性が高くなります。無線反射は、Wi-Fi 信号が壁、金属、ガラスなどの表面で反射し、マルチパス干渉を引き起こすときに発生します。これにより、信号品質が低下し、頻繁に切断される可能性があります。無線吸収、リピーターが多すぎる、クライアント接続が多すぎるなどの他の原因も Wi-Fi のパフォーマンスに影響しますが、反射面が多い環境では、過度の反射が一般的な原因となります。
参考: CompTIA Network+ 認定試験の目標 - ワイヤレス ネットワークのセクション。

最新問題**: 13**
VoIP 電話がポートに接続されていますが、通話を受信できません。この問題を解決するには、ポートで次のどれを実行する必要がありますか?
A. ポート上のすべての VLAN をトランクします。
B. ネイティブVLANを設定します。
C. トラフィックを音声 VLAN にタグ付けします。
D. VLAN を無効にします。
Answer: (解答を表示する**)**
VoIP と VLAN について理解する:
VoIP (Voice over IP) 電話では、パフォーマンスとセキュリティを向上させるために、音声トラフィックをデータ トラフィックから分離するために、VLAN (仮想ローカル エリア ネットワーク) がよく使用されます。
音声VLANへのトラフィックのタグ付け:
音声 VLAN の設定: スイッチのポートは、特定の音声 VLAN のトラフィックにタグを付けるように設定する必要があります。これにより、音声パケットが優先され、正しく処理されるようになります。
VLAN タグ付け: VLAN タグ付けにより、スイッチはネットワーク上の音声トラフィックを他の種類のトラフィックから識別して分離できるため、VoIP 通信の遅延とジッターが削減されます。
他のオプションとの比較:
ポート上のすべての VLAN をトランキングする: すべての VLAN のトランキングは、通常、個々のデバイス ポートではなく、スイッチ間のリンクに使用されます。
ネイティブ VLAN を設定します。ネイティブ VLAN はタグなしトラフィック用であり、音声トラフィックを分離して優先順位を付ける必要性には対応していません。
VLAN を無効にする: VLAN を無効にすると、音声トラフィックとデータ トラフィックが混在し、パフォーマンスの問題が発生したり、トラフィックが分離されなかったりする可能性があります。
実装：
VoIP 電話に接続されたスイッチ ポートを構成して、指定された音声 VLAN のトラフィックにタグを付け、適切なネットワーク セグメンテーションとサービス品質を確保します。
参照：
VLAN 構成と VoIP 実装に関する CompTIA Network+ 学習教材。

最新問題**: 14**
ユーザーは、リモート ファイル サーバーにアクセスできなくなったことをネットワーク管理者に通知します。ネットワーク管理者はサーバーに ping を実行し、現在のファイアウォール ルールがネットワーク ファイル共有へのアクセスをブロックしていないことを確認できます。

リモート ファイル サーバーで開いているポートを識別するのに役立つツールは次のどれですか。
A. 掘る
B. Nmap
C. トレース
D. nslookup
Answer: B (メーッセージを残す**)**
Nmap (Network Mapper) は、コンピュータ ネットワーク上のホストとサービスを検出するために使用される強力なネットワーク スキャン ツールです。リモート サーバーで開いているポートを識別するために使用でき、リモート ファイル サーバーなどのサービスへのアクセスの問題を診断するのに役立ちます。
* ポート スキャン: Nmap は包括的なポート スキャンを実行して、どのポートが開いているか、それらのポートでどのサービスが実行されているかを判別できます。
* ネットワーク検出: ホストのオペレーティング システム、サービス バージョン、ネットワーク構成に関する詳細情報を提供します。
* セキュリティ監査: トラブルシューティング以外にも、Nmap はセキュリティ監査や潜在的な脆弱性の特定にも使用されます。
ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: ネットワーク スキャン ツールとその使用方法について説明します。
* Nmap ドキュメント: 公式ドキュメントには、ポート スキャンとネットワーク診断に Nmap を使用する方法についての詳細な情報が記載されています。
* Network+ 認定オールインワン試験ガイド: Nmap を含むさまざまなネットワーク ユーティリティと、ネットワークのトラブルシューティングにおけるそれらのアプリケーションについて説明します。

最新問題**: 15**
次のどれが、単一のクラウド アカウント内でのコンピューティング リソースのセグメント化に最も関連していますか?
A. ネットワーク セキュリティ グループ
B. IaaS
C. ハイブリッドクラウド
D. VPC
Answer: D (メーッセージを残す**)**

最新問題**: 16**
サイト間接続を提供する最も安全な方法はどれですか?
A. VXLAN
B. IKE
C. GRE
D. IPsec
Answer: D (メーッセージを残す**)**
IPsec (インターネット プロトコル セキュリティ) は、サイト間接続を提供する最も安全な方法です。データの整合性、認証、暗号化などの堅牢なセキュリティ サービスが提供され、ネットワーク経由で送信されるデータが傍受や改ざんから保護されます。他のオプションとは異なり、IPsec はネットワーク層で動作し、IP ネットワークを通過するすべてのトラフィックを保護できるため、サイト間 VPN にとって最も包括的で安全な選択肢となります。参考資料:CompTIA Network+ 学習資料および NIST 特別出版物
800-77.

最新問題**: 17**
次の災害復旧の概念のうち、総稼働時間を総ユニット数で割って計算されるものはどれですか?
A. 平均所要時間
B. MTBF
C. RPO
D. RTO
Answer: B (メーッセージを残す**)**
災害復旧の概念の紹介:
災害復旧には、災害発生時に事業継続とデータ復旧を確保するための戦略と対策が含まれます。
平均故障間隔 (MTBF):
MTBF は、動作中のシステムの故障間隔を予測するために使用される信頼性メトリックです。総動作時間を故障数で割って計算されます。
計算式: MTBF = 総動作時間、故障数\text{MTBF} = \frac{\text{総動作時間}}{\text{故障数}}MTBF = 故障数、総動作時間 このメトリックは、システムとコンポーネントの信頼性と予想寿命を理解するのに役立ちます。
計算例:
サーバーが 1000 時間稼働し、2 回の障害が発生した場合、MTBF は次のようになります: MTBF=1000 時間2=500 時間\text{MTBF} = \frac{1000 \text{ 時間}}{2} = 500 \text{ 時間}MTBF=21000 時間=500 時間 オプションの説明:
A. MTTR (平均修復時間): 障害発生後にシステムを修復するのに必要な平均時間。
B. MTBF (平均故障間隔): 正解。故障間隔の平均時間を表します。
C. RPO (リカバリポイント目標): 時間で測定されたデータ損失の最大許容量。
D. RTO (目標復旧時間): 災害発生後の IT およびビジネス活動の復旧のために設定された目標時間。
結論：
MTBF は、災害復旧とシステムの信頼性における重要な指標であり、組織がメンテナンスを計画し、システム パフォーマンスを予測するのに役立ちます。
参照：
MTBF、MTTR、RPO、RTO の概念と計算について説明した CompTIA Network+ ガイド (Ref 10f 「Cisco Packet Tracer の使用方法」を参照)。

最新問題**: 18**
次のどれがサブインターフェースの使用を必要とする可能性が高いでしょうか?
A. 使用可能なLANポートが1つしかないルーター
B. ディープパケットインスペクションを実行するファイアウォール
C. ジャンボフレームを利用したハブ
D. スパニングツリープロトコルを使用するスイッチ
Answer: (解答を表示する**)**
* サブインターフェースの紹介:
* サブインターフェースは、単一の物理インターフェース上に作成される論理インターフェースです。ルーターが単一の物理インターフェース上で複数のネットワークをサポートできるようにするために使用されます。

* サブインターフェースの使用例:
* サブインターフェイスは、VLAN が実装されているシナリオでよく使用されます。単一の物理 LAN ポートを持つルータには、それぞれ異なる VLAN に関連付けられた複数のサブインターフェイスを設定できます。
* この設定により、ルータは異なる VLAN 間でトラフィックをルーティングできるようになります。
* 構成例:
* 単一の物理インターフェイス GigabitEthernet0/0 と 2 つの VLAN 10 および 20 を備えたルータを検討します。
インターフェース GigabitEthernet0/0.10
カプセル化 dot1Q 10
IPアドレス 192.168.10.1 255.255.255.0
！
インターフェース GigabitEthernet0/0.20
カプセル化 dot1Q 20
IPアドレス 192.168.20.1 255.255.255.0
* encapsulation dot1Q コマンドは VLAN ID を指定します。
* オプションの説明:
* A. 使用可能な LAN ポートが 1 つしかないルータ: 正解です。サブインターフェイスを使用すると、単一の物理インターフェイスで複数のネットワークを管理できるため、物理インターフェイスが限られているルータには不可欠です。
* B. ディープ パケット インスペクションを実行するファイアウォール: ファイアウォールはサブインターフェイスを使用できますが、ディープ パケット インスペクションの要件ではありません。
* C. ジャンボ フレームを利用するハブ: ハブはレイヤー 1 で動作し、IP アドレスを管理しないため、サブインターフェイスを使用しません。
* D. スパニングツリープロトコルを使用するスイッチ: STP は、ネットワーク内のループを防ぐためのプロトコルであり、サブインターフェイスを必要としません。
* 結論：
* サブインターフェイスは、物理インターフェイスが制限されたルータ上の複数の VLAN 間のルーティングに実用的なソリューションを提供します。これにより、ネットワーク管理者は利用可能なハードウェア リソースを効率的に使用できるようになります。
参考文献:
* CompTIA Network+ガイドでは、VLAN構成とサブインターフェースの使用について詳しく説明されています（参照ページ参照）。
9f基本設定コマンド)。

最新問題: **19**
次の攻撃のうち、複数のネットワーク タグを含むネットワーク パケットを利用するものはどれですか。
A. MACフラッディング
B. VLANホッピング
C. DNSスプーフィング
D. ARP ポイズニング
Answer: B (メーッセージを残す**)**
VLAN ホッピングは、攻撃者が複数の VLAN タグを持つパケットを作成し、VLAN 境界を不適切に通過できるようにする攻撃です。これにより、分離されているはずのネットワーク セグメントに不正アクセスされる可能性があります。その他のオプションでは、複数のネットワーク タグは使用されません。MAC フラッディングはスイッチの MAC アドレス テーブルを圧倒することを目的とし、DNS スプーフィングは DNS 応答を偽造し、ARP ポイズニングは偽の ARP メッセージを送信します。

最新問題: **20**
ゲスト ネットワークを使用する前に、管理者はユーザーに使用条件に同意することを要求します。この目的を達成するための最適な方法はどれですか。

A. 事前共有キー
B. 自律アクセスポイント
C. キャプティブポータル
D. WPA2 暗号化
Answer: C (メーッセージを残す**)**
キャプティブ ポータルは、ネットワークへのアクセスが許可される前にユーザーが表示して操作する必要がある Web ページです。
これは、ゲスト ネットワークで使用条件の同意を強制するためによく使用されます。ユーザーがネットワークに接続すると、このポータルにリダイレクトされ、続行する前に使用条件に同意する必要があります。この方法により、ユーザーがネットワークのポリシーを認識して同意していることが保証されるため、このシナリオでは最適な選択となります。参考資料: CompTIA Network+ 試験の目標と公式学習ガイド。

最新問題**: 21**
次のプロトコルのうち、ポート 22 を利用したリモート アクセスを提供するものはどれですか。
A. SSH
B. テルネット
C. TLS
D. RDP
Answer: A (メーッセージを残す**)**
SSH (Secure Shell) は、ネットワーク経由でリモート サーバー/システムに安全に接続するために使用するプロトコルです。ポート 22 で動作し、暗号化された通信を提供します。ポート 23 で動作し、安全ではない Telnet とは異なります。TLS は HTTP 接続 (HTTPS) のセキュリティ保護に使用され、ポート 443 などで動作します。一方、RDP (Remote Desktop Protocol) はリモート デスクトップ接続に使用され、ポート 3389 で動作します。
参照：
CompTIA Network+ の資料とチュートリアルでは、安全なリモート アクセスの標準プロトコルとしての SSH について説明し、ポート 22 での動作に重点を置いています。

最新問題**: 22**
ある会社のマーケティング チームが新しいアプリケーションを作成し、newapplication.comptia.org の DNS レコードを作成して、常に www.comptia.org と同じアドレスに解決したいと考えています。管理者は次のどのレコードを使用する必要がありますか。
A. SOA
B. MX
C. CNAME
D. NS
Answer: C (メーッセージを残す**)**
CNAME (正規名) レコードは、DNS でドメイン名を別のドメイン名にエイリアスするために使用されます。つまり、newapplication.comptia.org を www.comptia.org にポイントする CNAME レコードを作成することで、newapplication.comptia.org を www.comptia.org と同じ IP アドレスに解決できます。SOA (Start of Authority) は DNS ゾーン情報に使用され、MX (Mail Exchange) はメール サーバー レコードに使用され、NS (Name Server) は権威 DNS サーバーを指定するために使用されます。

最新問題**: 23**
次のどれがジャンボ フレームをサポートできますか?
A. アクセスポイント
B. ブリッジ
C. ハブ

D. スイッチ
Answer: (解答を表示する**)**
ジャンボ フレームの定義:
ジャンボ フレームは、1500 バイトを超えるペイロード (通常は最大 9000 バイト) を持つイーサネット フレームです。ジャンボ フレームは、小さいフレームによって発生するオーバーヘッドを削減することで、ネットワーク パフォーマンスを向上させるために使用されます。
スイッチがジャンボ フレームをサポートする理由:
スイッチは、データ パケットを管理するように設計されたネットワーク デバイスであり、ジャンボ フレームをサポートするように構成できます。この機能により、特に高性能ネットワークやデータ センターでスループットと効率が向上します。
他のデバイスとの非互換性:
アクセス ポイント: 主にワイヤレス通信を処理し、通常はジャンボ フレームをサポートしません。
ブリッジ: 異なるネットワーク セグメントを接続しますが、通常は標準のイーサネット フレーム サイズで動作します。
ハブ: デバイスを区別せずにすべてのポートにパケットを送信し、ジャンボ フレームを処理できない単純なネットワーク デバイス。
実用例:
スイッチでジャンボ フレームを有効にすると、ストレージ エリア ネットワーク (SAN) や大規模な仮想化環境など、大量のデータ転送が頻繁に行われる環境で役立ちます。
参照 :
CompTIA Network+ コース教材とネットワーク ハードウェア ドキュメント。

最新問題**: 24**
ネットワーク管理者は、システム イベントを相関させるために SIEM システムを実装したいと考えています。ネットワーク管理者は次のプロトコルのうちどれを検証する必要がありますか?
A. NTP
B. DNS
C. LDAP
D. DHCP
Answer: (解答を表示する**)**
NTP (ネットワーク タイム プロトコル) の役割:
NTP は、ネットワーク デバイスのクロックを基準時間ソースに同期するために使用されます。正確な時間同期は、さまざまなシステムからのイベントとログを相関させるのに不可欠です。
SIEM システムにとっての重要性:
イベント相関: SIEM (セキュリティ情報およびイベント管理) システムは、さまざまなソースからログ データを収集して分析します。複数のシステム間でイベントを相関させるには、正確なタイムスタンプが不可欠です。
時間の一貫性: 同期された時間がない状態では、インシデント発生時の一連のイベントをつなぎ合わせることが困難になり、法医学的分析が困難になります。
他のプロトコルとの比較:
DNS (ドメイン ネーム システム): ドメイン名を IP アドレスに変換しますが、時刻同期には関係ありません。
LDAP (Lightweight Directory Access Protocol): ユーザー認証や承認などのディレクトリ サービスに使用されます。
DHCP (Dynamic Host Configuration Protocol): ネットワーク上のデバイスに IP アドレスを割り当てますが、時刻の同期は処理しません。
実装 :
すべてのネットワーク デバイス、サーバー、エンドポイントが NTP を使用して同期されていることを確認します。これは、ローカル サーバーまたは外部のタイム ソースである NTP サーバーを使用するようにデバイスを構成することで実現できます。
参照 :
ネットワーク プロトコルと SIEM システムに関する CompTIA Network+ 学習教材。

最新問題: **25**
ネットワーク エンジニアが新しいメール サーバーへの移行を実行しました。エンジニアは MX レコードを変更し、変更が正確であることを確認し、A レコードの IP アドレス経由で新しいメール サーバーにアクセスできることを確認しました。ただし、ユーザーはメールを受信できません。問題の発生を防ぐためにエンジニアが実行すべきだったのは次のうちどれですか。
A. MX レコードと一致するように電子メール クライアントの構成を変更します。
B. MX レコードを変更する前に TTL レコードを減らします。
C. MX レコードを変更する前に DNS ゾーン転送を実行します。
D. IP アドレスの変更を反映するために NS レコードを更新します。
Answer: (解答を表示する**)**
* TTL (Time to Live) を理解する:
* TTL は DNS レコード内の値であり、DNS サーバーとクライアントによってレコードがキャッシュされる期間を示します。TTL 値が高いほど、レコードがより長くキャッシュされるため、DNS サーバーの負荷は軽減されますが、変更の伝播は遅れます。
* TTL による DNS 変更への影響:
* MX レコードを変更すると、TTL 設定により、変更がすべての DNS サーバーに反映されるまでに時間がかかる場合があります。TTL が高いと、古い DNS 情報がキャッシュされたままになり、メールが古いサーバーに送信される可能性があります。
* DNSを変更する前のベストプラクティス:
* DNS レコードへの変更が迅速に伝播されるようにするには、変更を行う前に TTL 値を低い値 (300 秒や 5 分など) に減らすことをお勧めします。
これにより、キャッシュされたレコードはすぐに期限切れになり、新しいレコードがより早く使用されるようになります。
* DNS変更の検証:
* TTL を減らして MX レコードを変更した後は、digornslookup などのツールを使用して伝播を確認することが重要です。
* 他のオプションとの比較:
* MX レコードと一致するように電子メール クライアントの構成を変更します。通常、電子メール クライアントは MX レコードと直接一致する必要はありません。通常は、設定で指定された特定のメール サーバーに接続します。
* MX レコードの変更前に DNS ゾーン転送を実行します。DNS ゾーン転送は、DNS サーバー間で DNS レコードを複製するために使用されますが、個々のレコードの変更の伝播とは関係ありません。
* IP アドレスの変更を反映するように NS レコードを更新します。NS レコードはドメインの DNS サーバーを指定するものであり、MX レコードの変更とは関係ありません。
参考文献:
* CompTIA Network+ の学習教材と DNS のベスト プラクティス。

最新問題: **26**
ネットワーク管理者は、2 台のルーターをポイントツーポイント構成で接続し、IP スペースを節約する必要があります。
管理者は次のサブネットのどれを使用する必要がありますか?
A. 724
B. /26
C. /28
D. /30
Answer: D (メーッセージを残す**)**
/30 サブネット マスクの使用は、2 台のルータ間のポイントツーポイント接続の IP スペースを節約する最も効率的な方法です。/30 サブネットは 4 つの IP アドレスを提供し、そのうち 2 つはルータ インターフェイスに、1 つはネットワーク アドレスに、もう 1 つはブロードキャスト アドレスに割り当てることができます。このため、使用可能な IP アドレスが 2 つだけ必要なポイントツーポイント リンクに最適です。参考資料:CompTIA Network+ 学習教材およびサブネット化の原則。

最新問題: **27**

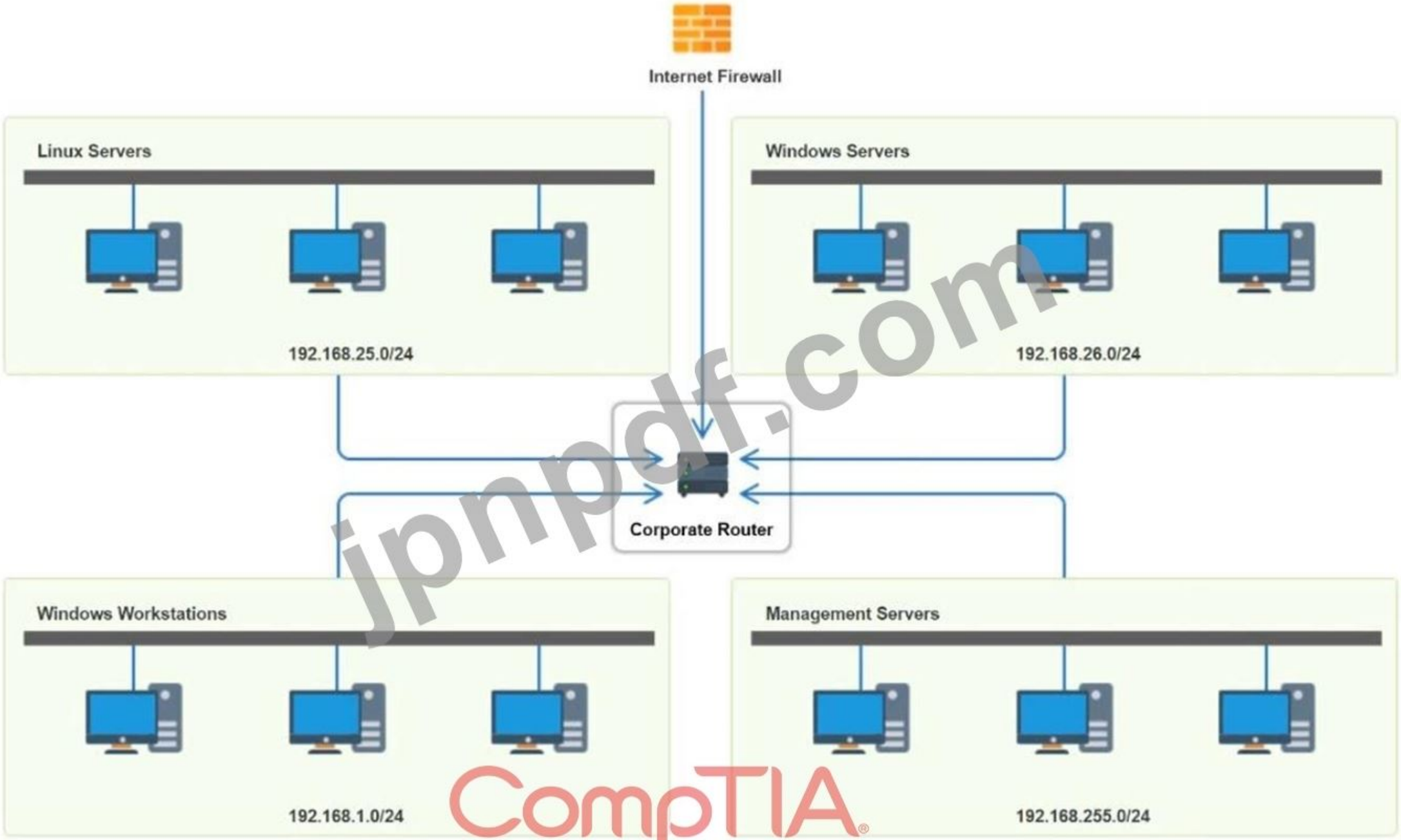
次のネットワーク ケーブルのうち、保護被覆から光を反射するものはどれですか。
A. ツインアキシャル
B. 同軸
C. シングルモード
D. マルチモード
Answer: (解答を表示する**)**
マルチモード光ファイバーケーブルでは、光ファイバーを伝わる際にコアのクラッドで反射した光信号が伝送されます。この特性は、光がクラッドで反射することなく光ファイバーを直接伝わるシングルモード光ファイバーと異なります。
マルチモード ファイバー ケーブルに関する詳細なポイントは次のとおりです。
* 構造: マルチモード ファイバーのコア径は、シングルモード ファイバーのコア径 (約 9 ミクロン) に比べて大きく、通常は 50 または 62.5 ミクロンです。
* 光の伝播: マルチモード ファイバーのコアが大きいため、複数の光モードが伝播します。これらのモードはさまざまな角度で伝搬し、コアとクラッドの境界で反射します。
* 距離と帯域幅: モード分散により、異なる光モードが受信機に到達するタイミングが
* さまざまな場合、マルチモード ファイバーはシングルモード ファイバーに比べて短距離のアプリケーションに適しています。OM4 マルチモード ファイバーを使用した 10 Gbps イーサネットの場合、一般的な距離は最大 550 メートルです。
* 用途: マルチモード ファイバーは、コスト効率と設置の容易さから、LAN (ローカル エリア ネットワーク)、データ センター、短距離データ伝送によく使用されます。
ネットワーク参照:
* マルチモード ファイバーとシングルモード ファイバーの違いなど、光ファイバー技術について説明した CompTIA Network+ N10-007 公式認定ガイド。
* Cisco Networking Academy: さまざまな光ファイバーケーブルの特性に関するトレーニング資料とリファレンス ガイドを提供します。
* 光ファイバー協会 (FOA): 光ファイバーに特化した専門団体で、光ファイバー技術に関する広範な情報と認定を提供しています。
マルチモード ファイバーは、高データ レートの短距離通信用に特別に設計されており、通常、短距離での高帯域幅が重要なデータ センターなどの環境で使用されます。マルチモード ファイバーに固有のクラッドからの反射により、この大容量通信が可能になります。

最新問題: **28**
組織のアーキテクチャに OT デバイスを追加するときに、ネットワーク管理者は次のどれを設定する必要がありますか?
A. ハニーネット
B. 保存データの暗号化
C. ネットワークセグメンテーション
D. 時間ベースの認証
Answer: C (メーッセージを残す**)**

最新問題: **29**
設置するラックのサイズを決定する要因として最も可能性が高いのはどれですか (2 つ選択してください)。
A. KVMのサイズ
B. スイッチの深さ
C. ハードドライブのサイズ
D. 冷却ファンの速度
E. コンセントのアンペア数
F. サーバーの高さ
Answer: (解答を表示する**)**
* ラックサイズの決定について理解する:

※設置するラックのサイズは、ラックに収納する機器の寸法、主に奥行きと高さによって決まります。
* スイッチの深さ:
* 機器の奥行き: ネットワーク スイッチやその他のラック マウント デバイスの奥行きは、ラックの奥行きに直接影響します。機器の奥行きが深い場合は、それを収容するためにより深いラックが必要になります。
* 業界標準: ほとんどのラックは標準的な奥行きで提供されますが、適切なフィット感と空気の流れを確保するには、ラックの奥行きを機器の最も深い部分に合わせて調整することが重要です。
* サーバーの高さ:
* 機器の高さ: サーバーやその他のデバイスの高さはラック ユニット (U) で測定され、1U は 1.75 インチに相当します。すべての機器の合計高さによって、ラックの全体的な高さ要件が決まります。
* ラック ユニット: ラックの高さは通常、42U、48U など、収容できるラック ユニットの数で表されます。
* 他のオプションがあまり重要でない理由:
* KVM サイズ: 管理には重要ですが、KVM (キーボード、ビデオ、マウス) スイッチは通常、ラック サイズを決定するものではありません。
* ハード ドライブのサイズ: 個々のハード ドライブはサーバーまたはストレージ デバイス内にインストールされ、ラックの寸法に直接影響しません。
* 冷却ファンの速度: ファンの速度は冷却に影響しますが、ラックの物理的なサイズには影響しません。
* コンセントのアンペア数: 電力要件はラックの寸法を決定するのではなく、ラックをサポートする電気インフラストラクチャによって決まります。
参考文献:
* ラックの設置と機器のサイズ設定に関する CompTIA Network+ の学習教材。

最新問題**: 30**
ルータに次の ACL を実装することが求められています。
1. 管理ネットワークから他のすべてのローカルネットワークセグメントへの最も一般的に使用される安全なリモートアクセステクノロジを許可する
2. ユーザー サブネットが、Linux および Windows Server セグメントで最も一般的に使用されるリモート アクセス テクノロジを使用できないことを確認します。
3. 特に許可されていないトラフィックを禁止します。
説明書
ドロップダウンを使用してACLを完了します
いつでもシミュレーションの初期状態に戻したい場合は、すべてリセット」ボタンをクリックしてください。



Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0	192.168.1.0 192.168.25.0	Any	SSH Telnet	Allow Deny

	192.168.255.0 192.168.26.0 Any	192.168.255.0 192.168.26.0 Any		Telnet HTTP RDP VNC SMB Any	Deny

Answer:

答えと解決策は下記をご覧ください。

Explanation:

Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

最新問題: **31**

提供された URL が正しい IP アドレスに解決されないため、ユーザーは Web サイトに移動できません。他のユーザーは問題なく目的の Web サイトに移動できます。この問題の原因として最も可能性が高いのは次のどれですか。

A. ホストファイル

B. 自己署名証明書

C. ネームサーバーレコード

D. IP ヘルパー

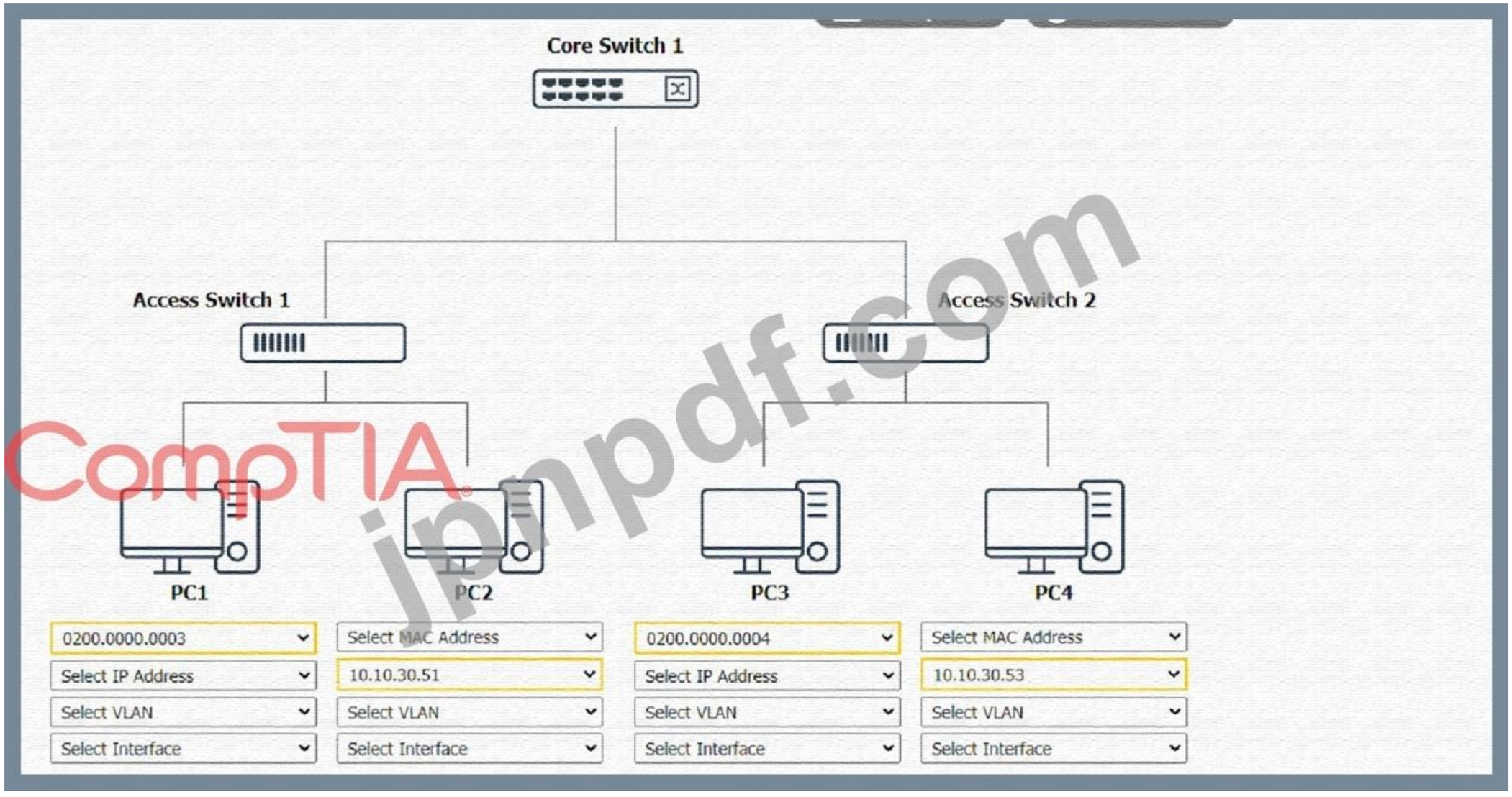
Answer: (解答を表示する**)**

年

Explanation:

Hosts ファイルの役割:
hosts ファイルは、ホスト名を IP アドレスにマッピングするコンピュータ上のローカル ファイルです。ホスト名を IP アドレスに静的にマッピングすることで、DNS 解決をオーバーライドするために使用できます。
Hosts ファイルに関する一般的な問題:
ホスト ファイル内のホスト名に誤った IP アドレスがマップされている場合、コンピューターがホスト名を誤った IP アドレスに解決する可能性があります。これにより、特定の Web サイトでナビゲーションの問題が発生する可能性がありますが、DNS に依存している他のユーザーには同じ問題はありません。
他の選択肢の可能性が低い理由:
自己署名証明書: SSL/TLS に関連し、ナビゲーションの失敗ではなく、セキュリティ警告が発生します。
ネームサーバー レコード: 1 人のユーザーだけでなく、すべてのユーザーに影響します。
IP ヘルパー: DHCP 要求を転送するために使用され、DNS 解決の問題とは無関係です。
トラブルシューティングの手順:
影響を受けるユーザーのコンピューター上の hosts ファイルを確認します (Windows の場合は C:\Windows\System32\drivers\etc\hosts、Unix/Linux の場合は /etc/hosts)。
問題のあるホスト名を誤った IP アドレスにマッピングするエントリを探し、修正または削除します。
参照：
CompTIA Network+ の学習教材とシステム管理ドキュメント。

最新問題: 32
最近、ネットワーク技術者が会社に入社しました。マネージャーは、ネットワークの文書化を技術者に任せ、以前の文書から部分的な情報を技術者に提供しました。
説明書：
各スイッチをクリックし、ターミナルにコマンドを入力してネットワーク検出を実行します。提供されているドロップダウン メニューを使用して、不足している情報を入力します。




Core Switch 1 Prompt
C:\> nmap
% Invalid input detected.
C:\> netdiscover
% Invalid input detected.
C:\>
jpnpdf.com
CompTIA.

Answer:

このシミュレーションの詳細については説明を参照してください。

Explanation:

(注: Ips は各シミュレーション タスクで変更されるため、理解を深めるために回答例を示します) ターミナルにコマンドを入力してネットワーク検出を実行するには、次の手順に従います。

* 各スイッチをクリックすると、ターミナル ウィンドウが開きます。
* スイッチ インターフェイスの IP アドレスとステータスを表示するには、show ip interface Brief コマンドを入力します。
* スイッチ インターフェイスの VLAN 設定と割り当てを表示するには、show vlan Brief コマンドを入力します。
* スイッチに接続されている隣接デバイスに関する情報を表示するには、show cdp neighbors コマンドを入力します。
* 提供されているドロップダウン メニューを使用して、図に不足している情報を入力します。

コア スイッチ 1 の不足している情報を入力する方法の例を次に示します。

* コアスイッチ1のIPアドレスは192.168.1.1です。
* コアスイッチ1のVLAN構成は、VLAN 1: 192.168.1.0/24、VLAN 2: 192.168.2.0/24、VLAN 3: 192.168.3.0/24です。
* コア スイッチ 1 の隣接デバイスは、アクセス スイッチ 1 とアクセス スイッチ 2 です。
* コア スイッチ 1 をアクセス スイッチ 1 に接続するインターフェイスは、GigabitEthernet0/1 と GigabitEthernet0/2 です。
* コア スイッチ 1 とアクセス スイッチ 2 を接続するインターフェイスは、GigabitEthernet0/3 と GigabitEthernet0/4 です。

同じ手順を使用して、アクセス スイッチ 1 とアクセス スイッチ 2 の不足している情報を入力できます。

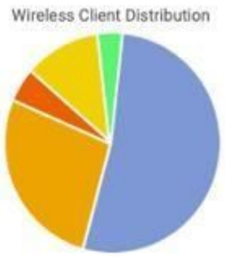
最新問題: **33**
最近の侵害を受けて、クライアントは全体的なセキュリティを強化したいと考えています。次のうち、実装するのに最適なものはどれですか? (2 つ選択してください。)
A. 最小権限のネットワークアクセス
B. 動的在庫
C. 集中ポリシー管理
D. ゼロタッチプロビジョニング
E. 構成ドリフト防止
F. サブネット範囲の制限
Answer: A,C (メーッセージを残す**)**
最近の侵害後に全体的なセキュリティを強化するには、最小権限のネットワーク アクセスと集中ポリシー管理を実装することが効果的な戦略です。
* 最小権限ネットワーク アクセス: この原則により、ユーザーとデバイスには機能を実行するために必要なアクセスのみが付与され、不正アクセスや侵害の可能性が最小限に抑えられます。権限を制限することで、攻撃者がネットワークの重要な部分にアクセスするリスクが軽減されます。
* 集中ポリシー管理: セキュリティ ポリシーを集中管理することで、ネットワーク全体にわたってセキュリティ対策を一貫して効率的に実装できます。これにより、セキュリティ インシデントに迅速に対応し、セキュリティ プロトコルに準拠し、誤った構成が発生する可能性を減らすことができます。
ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: 最小権限やポリシー管理などのネットワーク セキュリティの原則について説明します。
* Cisco Networking Academy: セキュリティ ポリシーとアクセス制御の実装に関するトレーニングを提供します。
* Network+ 認定オールインワン試験ガイド: ネットワーク セキュリティを強化し、ポリシーを効果的に管理するための戦略について説明します。

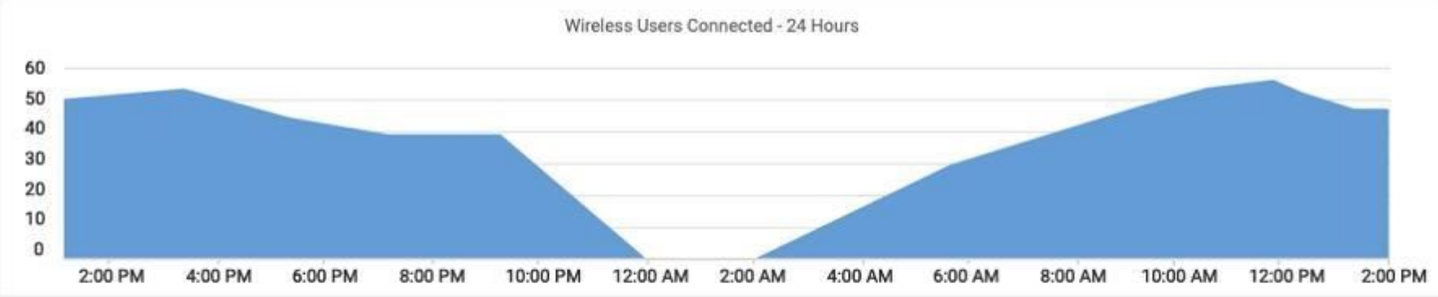
最新問題: **34**
ユーザーは Web ブラウザ経由で企業の VPN に接続し、TLS を使用して社内財務システムにアクセスし、タイムカードを入力できます。VPN の使用方法を最もよく表しているのは次のどれですか。
A. サイト間
B. クライアントレス
C. クライアントからサイトへ
D. フルトンネル
Answer: B (メーッセージを残す**)**

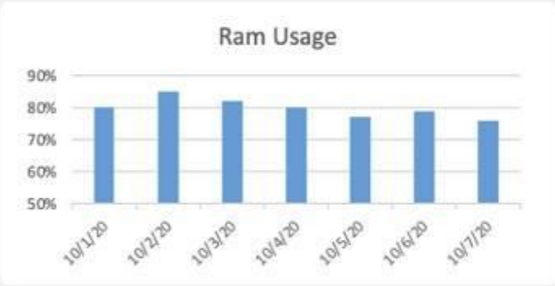
最新問題: **35**
最近の停電後、アプリケーション サーバーへのアクセスでパフォーマンスの問題がユーザーから報告されています。ワイヤレス ユーザーからも、インターネットが断続的に切断される問題が報告されています。
説明書
画面上部の各タブをクリックします。情報を表示するウィジェットを選択し、ドロップダウン メニューを使用して関連する質問に回答します。いつでもシミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。

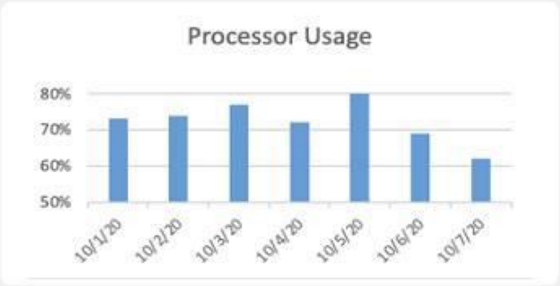
Network Health | Device Monitoring

Show Question | Reset All Answers









Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

Which WAN station should be preferred for VoIP traffice?

WAN 1

Select WAN
WAN 1
WAN 2

Network Health | Device Monitoring

Show Question | Reset All Answers

Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb

Up (8)

Warning (2)

Down (1)

3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues?

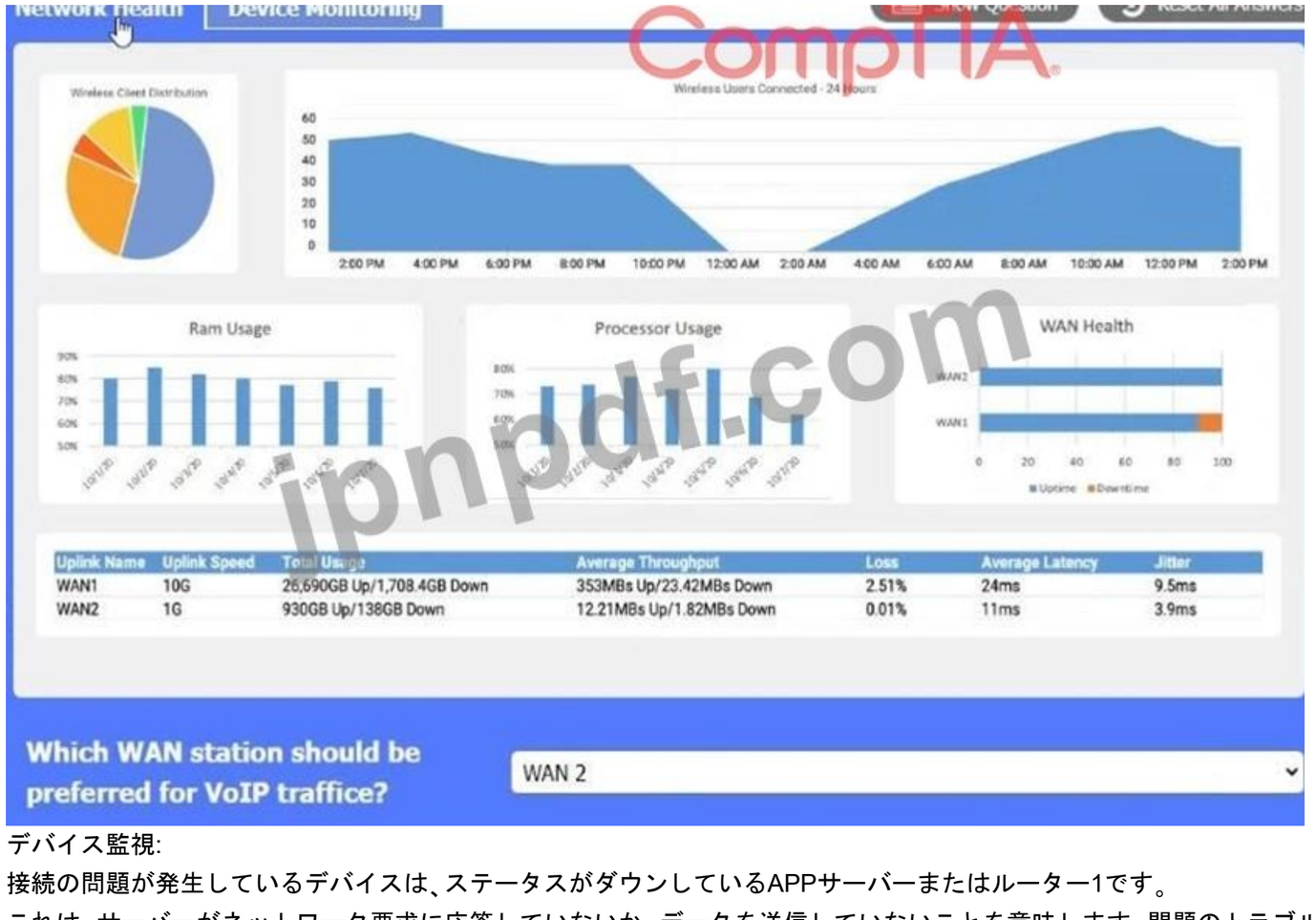
Select Answer
Router A
Router B
WAP1
WAP2
WirelessController
Switch A
Switch B
DHCP Server
Web Server
APP Server

Router A

Which workstation IP is generating the MOST traffic?

Select Answer
10.1.99.28
10.1.99.14
10.1.99.10
10.1.99.22
10.1.99.24
206.208.133.10
206.208.133.9
10.1.50.14
10.1.50.13
10.1.59.81

Answer:
答えと解決策は下記をご覧ください。
Explanation:
ネットワークの健全性:
WAN 2 は平均遅延と損失率が低いため、VoIP トラフィックに適した WAN ステーションになります。VoIP トラフィックでは、良好な音声品質と信頼性を確保するために、遅延とパケット損失を低く抑える必要があります。WAN 1 は RAM とプロセッサの使用率が高いため、VoIP トラフィックのパフォーマンスにも影響する可能性があります。
提供された画像からの WAN 1 と WAN 2 の主要なメトリックの概要は次のとおりです。
* WAN1:
* アップリンク速度: 10G
* 総使用量: アップロード 26.969GB / ダウン 1.748GB
* 平均スループット: 353MBps アップ / 23.42MBps ダウン
* 損失: 2.51%
* 平均遅延: 24ms
* ジッター: 9.5ms
* WAN 2:
* アップリンク速度: 1G
* 合計使用量: 930GB アップロード / 138GB ダウン
* 平均スループット: 12.21MBps 上り / 1.82MBps 下り
* 損失: 0.01%
* 平均遅延: 11ms
* ジッター: 3.9ms
VoIP トラフィックの場合、音声品質を確保するには、低遅延と低ジッターが特に重要です。WAN 1 は帯域幅とスループットが高いですが、WAN 2 と比較して遅延とジッターも高くなっています。ただし、WAN 2 は損失、遅延、ジッターがはるかに低く、遅延やパケット到着時間の変動に敏感な VoIP トラフィックに適しています。
この情報を考慮すると、WAN 2 は、WAN 1 と比較して帯域幅が低いにもかかわらず、遅延が少なく、ジッターが少なく、損失率が大幅に低いため、VoIP トラフィックに一般的に好まれます。WAN 1 の高帯域幅は、バルク データ転送など、遅延やジッターの影響を受けにくい他の種類のトラフィックに適している可能性があります。



デバイス監視:
接続の問題が発生しているデバイスは、ステータスがダウンしているAPPサーバーまたはルーター1です。
これは、サーバーがネットワーク要求に応答していないか、データを送信していないことを意味します。問題のトラブルシューティングを行うには、APP サーバーの物理的な接続、電源、および構成を確認することをお勧めします。

最新問題: **36**
ネットワーク管理者は、2 台のルーターをポイントツーポイント構成で接続し、IP スペースを節約する必要があります。管理者は次のどのサブネットを使用する必要がありますか?
A. 724
B. /26
C. /28
D. /30
Answer: D (メーッセージを残す**)**
/30 サブネット マスクの使用は、2 台のルータ間のポイントツーポイント接続の IP スペースを節約する最も効率的な方法です。/30 サブネットは 4 つの IP アドレスを提供し、そのうち 2 つはルータ インターフェイスに、1 つはネットワーク アドレスに、もう 1 つはブロードキャスト アドレスに割り当てることができます。このため、使用可能な IP アドレスが 2 つだけ必要なポイントツーポイント リンクに最適です。
参考: CompTIA Network+ の学習教材とサブネット化の原則。

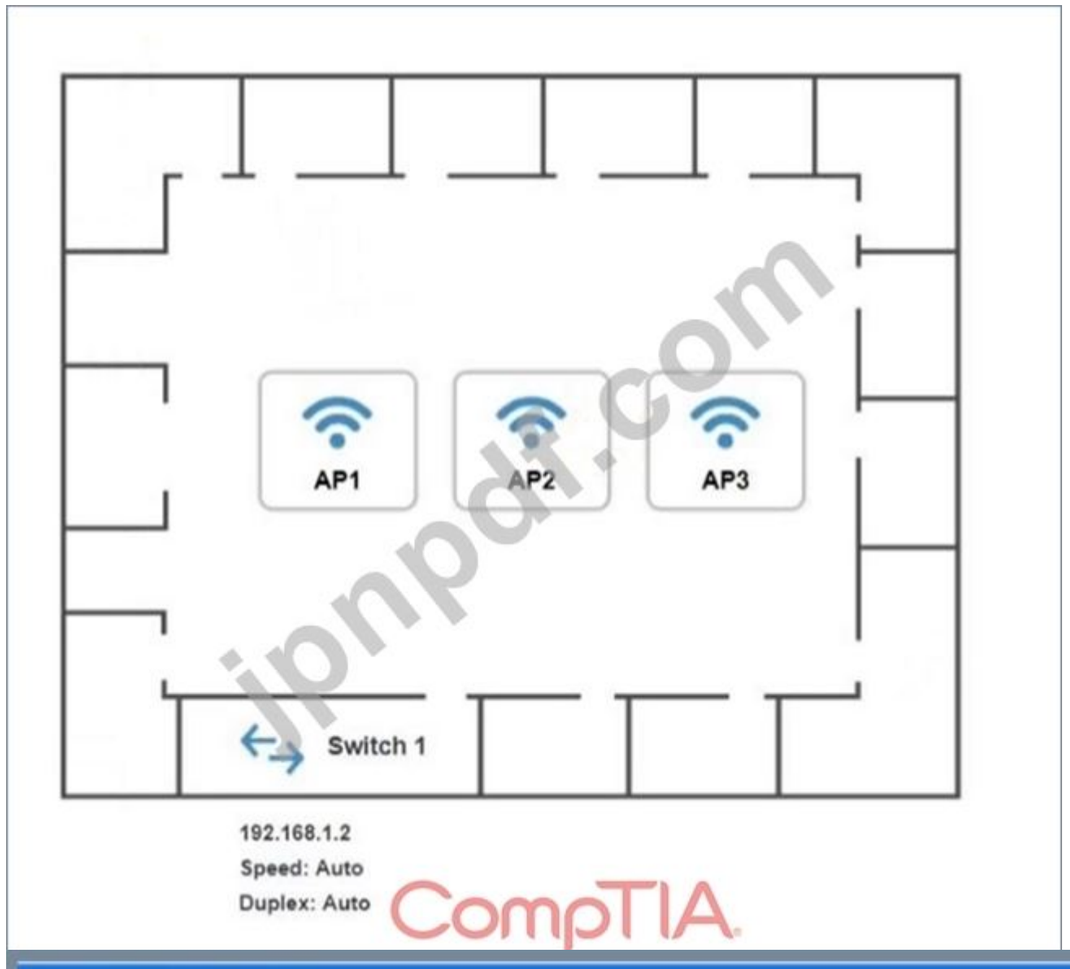
最新問題: **37**
ネットワーク管理者は各部門にセキュリティ ゾーンを実装しています。このタスクを実行するために管理者は次のどれを使用する必要がありますか?
A. ACL
B. ポートセキュリティ
C. コンテンツフィルタリング
D. NAC
Answer: A (メーッセージを残す**)**

* ACL を理解する:
* アクセス制御リスト (ACL): IP アドレス、プロトコル、またはポートに基づいてパケットをフィルタリングすることにより、ネットワーク トラフィックを制御し、ネットワーク リソースへのアクセスを制限するために使用される一連のルール。
* セキュリティゾーンの実装:
* ゾーンの定義: ACL を使用すると、さまざまな部門に特定のルールを適用してセキュリティ ゾーンを作成し、これらのゾーン間で許可されたトラフィックのみが許可されるようにすることができます。
* トラフィックの制御: ACL はネットワーク境界で受信トラフィックと送信トラフィックを制御し、セキュリティ ポリシーを適用して不正アクセスを防止します。
* 他のオプションとの比較:
* ポート セキュリティ: スイッチ ポートに接続できるデバイスの数を制限し、MAC アドレス フラッディング攻撃を防止しますが、セキュリティ ゾーンの定義には使用されません。
* コンテンツ フィルタリング: 事前定義されたポリシーに基づいて特定のコンテンツへのアクセスをブロックまたは許可します。通常は、ネットワーク セグメンテーションではなく Web フィルタリングに使用されます。
* NAC (ネットワーク アクセス制御): デバイスのセキュリティ状態に基づいてネットワークへのアクセスを制御しますが、セキュリティ ゾーンは定義しません。
* 実装手順:
* 各部門の要件に基づいて ACL ルールを定義します。
* これらのルールを適切なネットワークインターフェースまたはファイアウォールポリシーに適用して、ネットワークをセグメント化します。
* セキュリティゾーン内へ。
参考文献:
* ネットワーク セキュリティとアクセス制御方法に関する CompTIA Network+ 学習教材。

最新問題**: 38**
次の IP 送信タイプのうち、送信されるデータをすべて暗号化するものはどれですか?
A. 超能力
B. あぁ
C. GRE
D. UDP
E. TC
Answer: (解答を表示する**)**
ポ
Explanation:
ESP (Encapsulating Security Payload) の定義:
ESP は、データの機密性、整合性、および信頼性を提供するために使用される IPsec プロトコル スイートの一部です。ESP は、ペイロードとオプションの ESP トレーラーを暗号化し、データの機密性を提供します。
ESP 機能:
ESP は IP パケット全体を暗号化し、パケット内のデータが傍受や盗聴から保護されることを保証します。また、データの整合性と認証のオプションも提供します。
ESP は、トランスポート モード (IP パケットのペイロードのみを暗号化) とトンネル モード (IP パケット全体を暗号化) の 2 つのモードで動作します。
他のプロトコルとの比較:
AH (認証ヘッダー): データの整合性と認証を提供しますが、ペイロードは暗号化しません。
GRE (Generic Routing Encapsulation): 暗号化を提供しないトンネリング プロトコル。
UDP (ユーザー データグラム プロトコル) と TCP (伝送制御プロトコル): これらは、本質的に暗号化を提供しないトランスポート層プロトコルです。暗号化は、TLS/SSL などの追加プロトコルによって提供する必要があります。
使用例:

ESP は、インターネットなどの信頼できないネットワーク上で安全な通信を確保するために、VPN (仮想プライベート ネットワーク) で広く使用されています。
参照：
IPsec と暗号化に関する CompTIA Network+ 学習教材。

最新問題: **39**
シミュレーション
オフィスにワイヤレス ネットワークを設定するという任務を負っています。ネットワークは 3 つのアクセス ポイントと 1 つのスイッチで構成されます。ネットワークは次のパラメータを満たす必要があります。
SSID は、S3cr3t のキーを使用して CorpNet として設定する必要があります。
無線信号は互いに干渉し合ってはならない
アクセス ポイントとスイッチが接続されているサブネットは、最大 30 台のデバイスのみをサポートする必要があります。アクセス ポイントは、TKIP クライアントを最大速度でのみサポートするように構成する必要があります。手順: ワイヤレス デバイスをクリックしてその情報を確認し、アクセス ポイントの設定を特定の要件に合わせて調整します。
いつでもシミュレーションの初期状態に戻したい場合は、 すべてリセット」ボタンをクリックしてください。



https://ap1.setup.do

Basic Configuration

Access Point Name AP1

IP Address /

Gateway 192.168.1.1

SSID

SSID Broadcast Yes No

Wireless

Mode

B
G

Channel

Wired

Speed Auto 100 1000

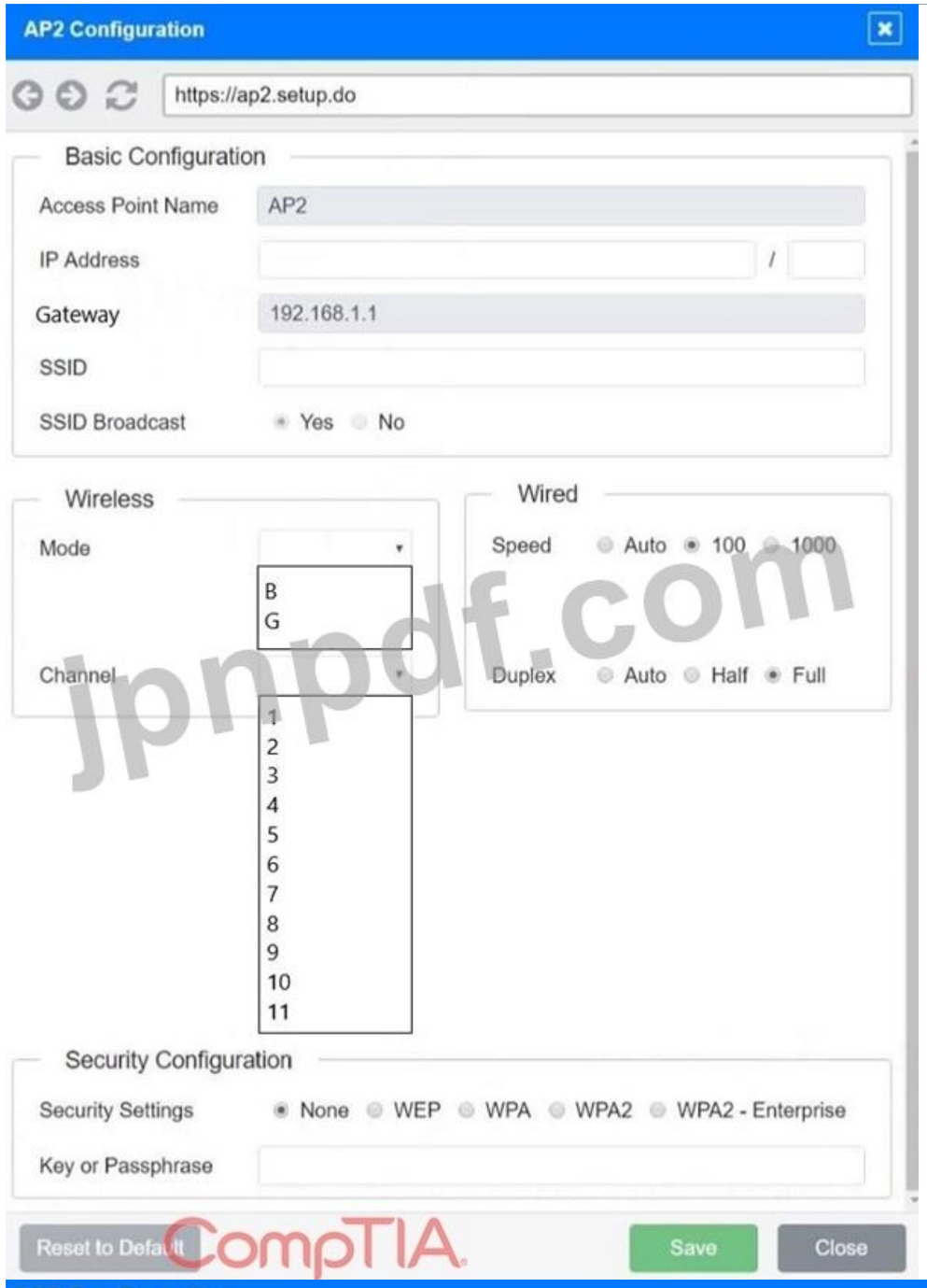
Duplex Auto Half Full

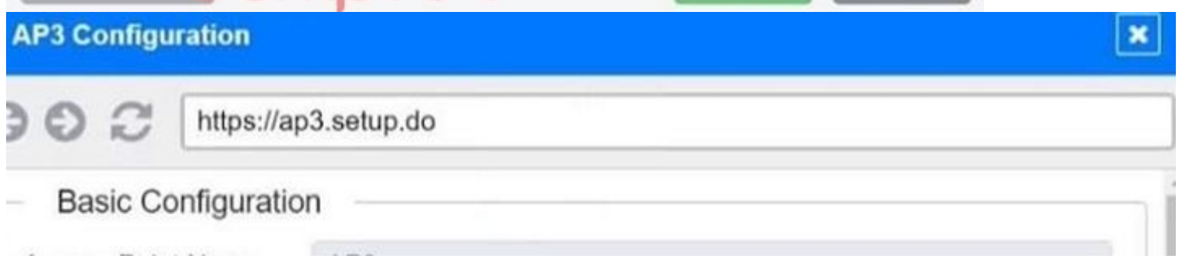
Security Configuration

Security Settings None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase

Reset to Default Save Close



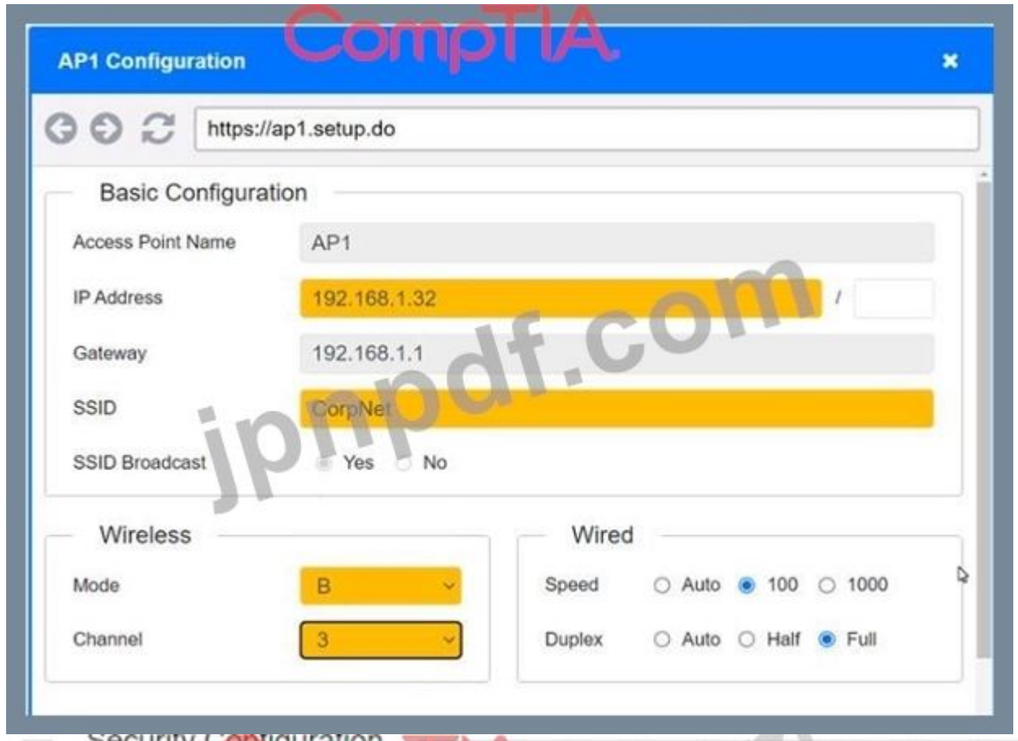


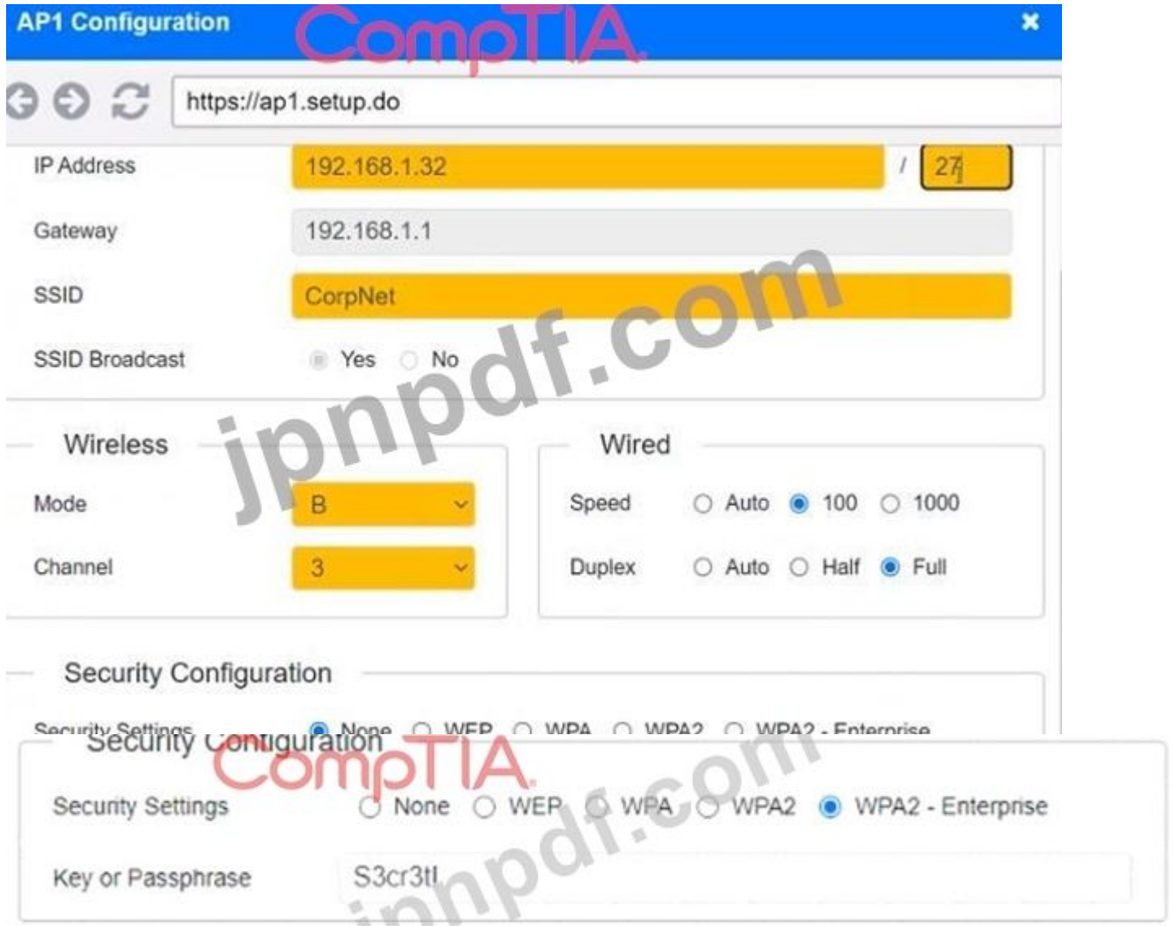
Answer:

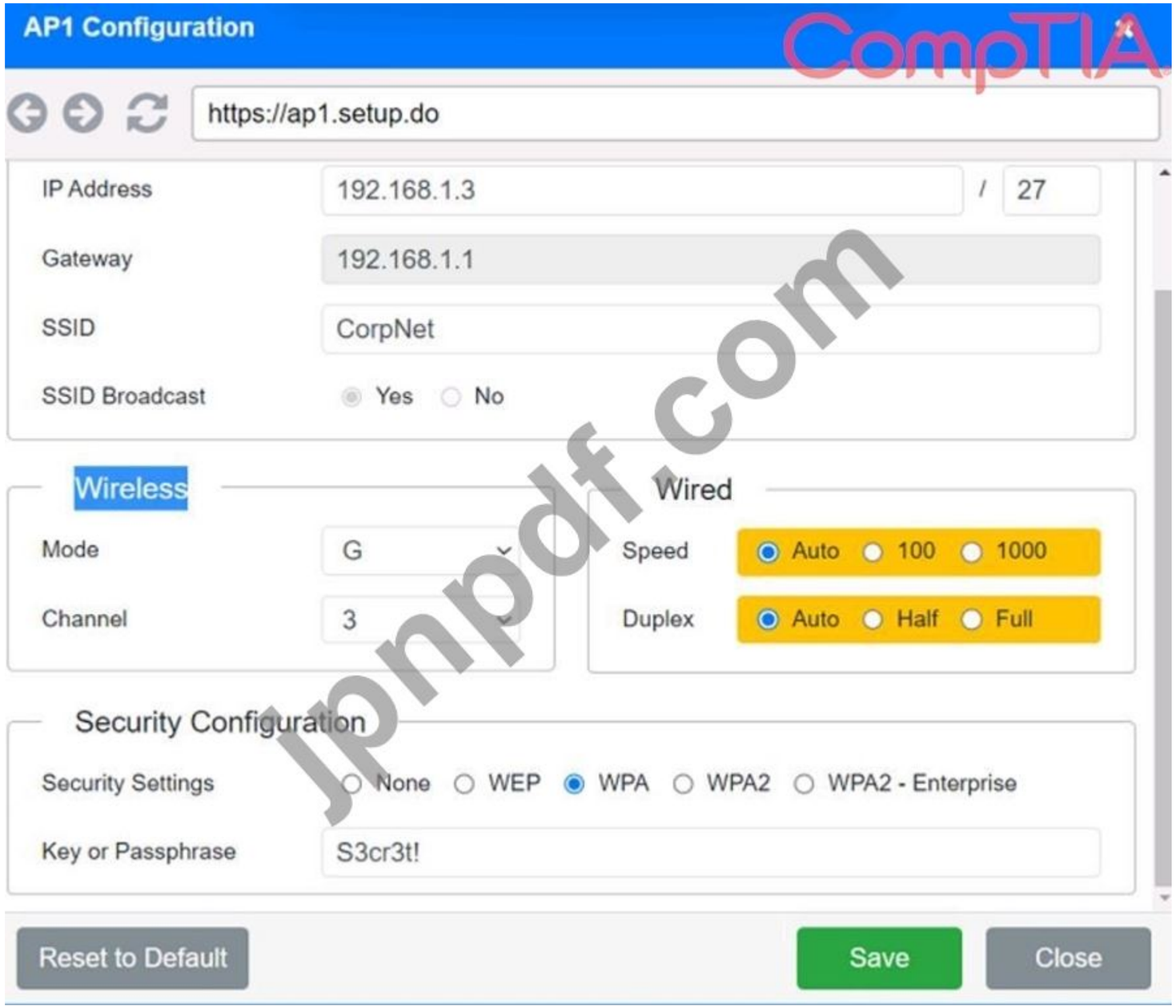
下記の説明を参照してください。

Explanation:

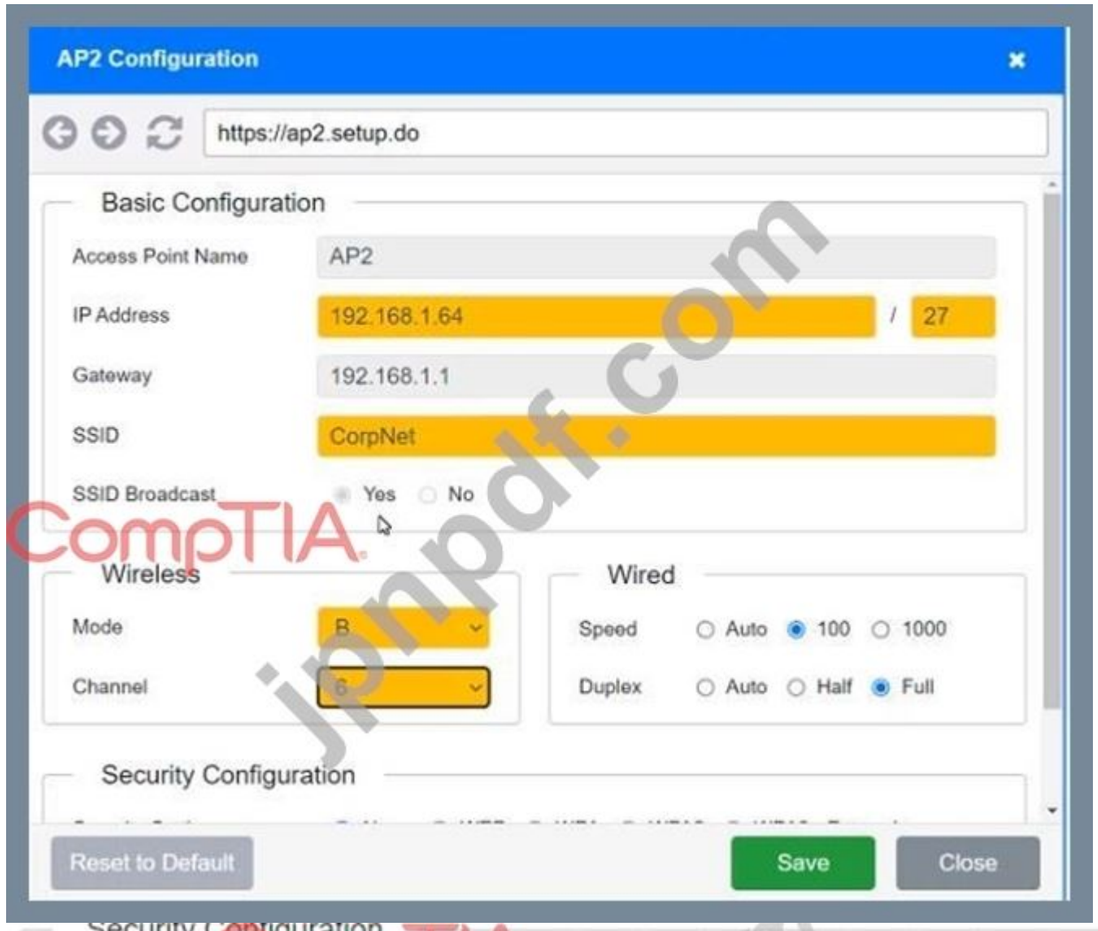
最初の展示では、レイアウトは次のようになります




AP1 Configuration
https://ap1.setup.do
IP Address
192.168.1.32
/
27
Gateway
192.168.1.1
SSID
CorpNet
SSID Broadcast
Yes
No
Wireless
Mode
B
Channel
3
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
S3cr3tI



別紙2は以下のとおり
アクセスポイント名 AP2



別添3は以下のとおり
アクセスポイント名 AP3

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name: AP3

IP Address: 192.168.1.96 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: Yes No

Wireless

Mode: B

Channel: 9

Wired

Speed: Auto 100 1000

Duplex: Auto Half Full

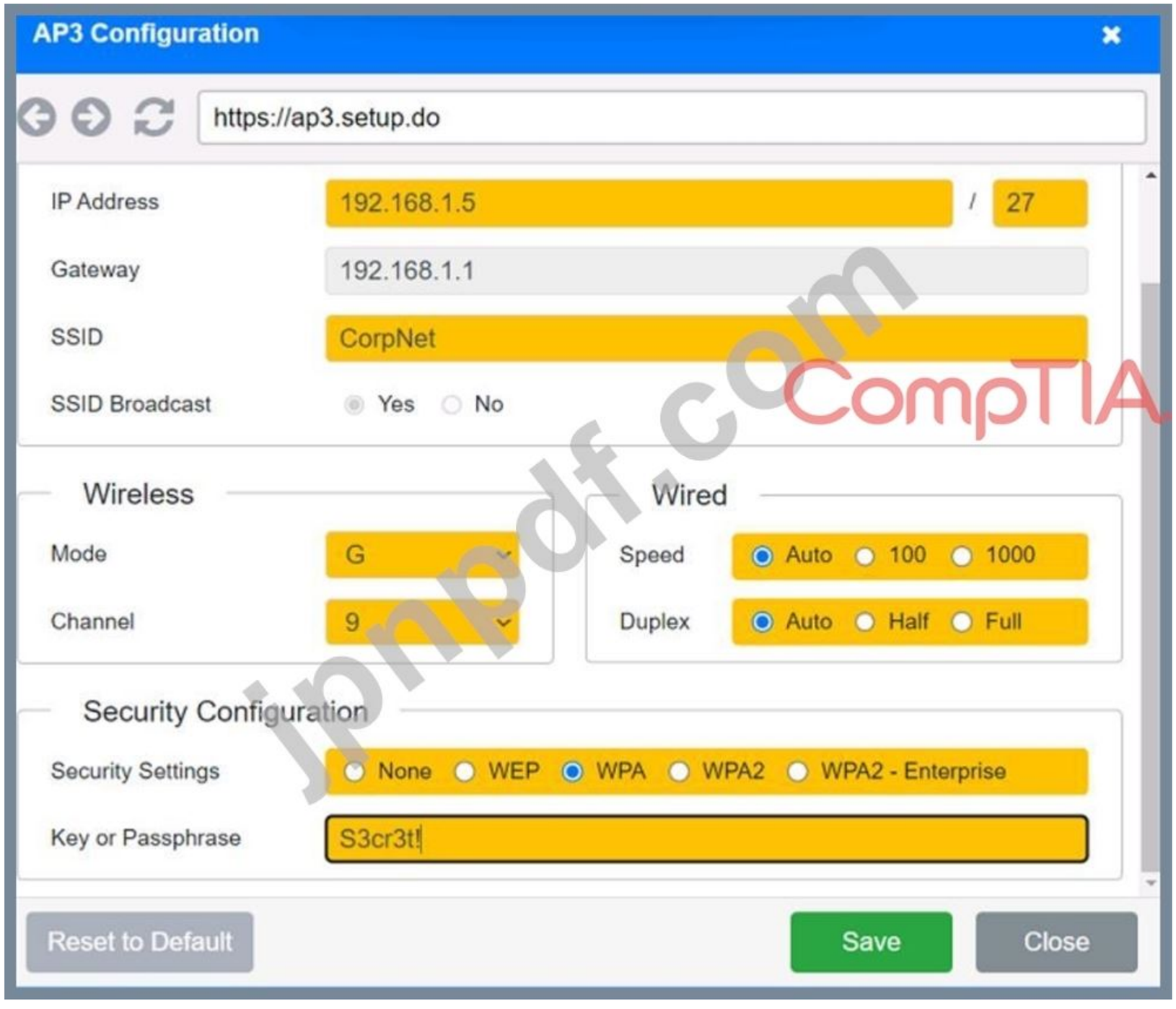
Security Configuration

Reset to Default | Save | Close

Security Configuration

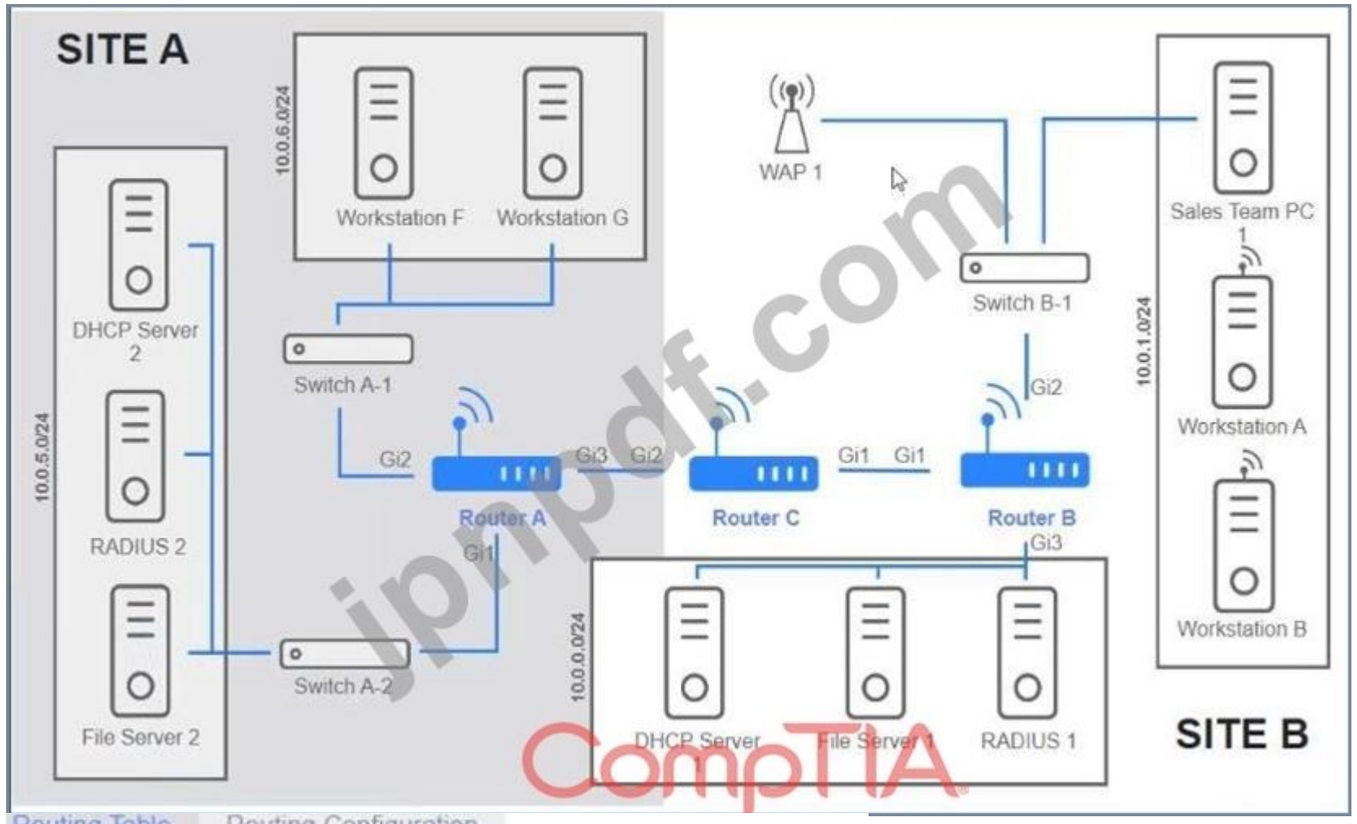
Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase: S3cr3t!



最新問題: **40**
ユーザーは、ファイル サーバー 2 にある部門共有のファイルにアクセスできません。ネットワーク管理者は、ワークステーション A とファイル サーバー 2 をホストするネットワーク間のルーティングを検証する役割を担っています。
説明書
各ルータをクリックして出力を確認し、問題を特定し、適切なソリューションを構成します。いつでもトライシミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてくだ

さい。




```
Router-B# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, GigabitEthernet1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/22 is directly connected, GigabitEthernet3
L        10.0.0.1/32 is directly connected, GigabitEthernet3
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.5/32 is directly connected, GigabitEthernet1
```

Answer:

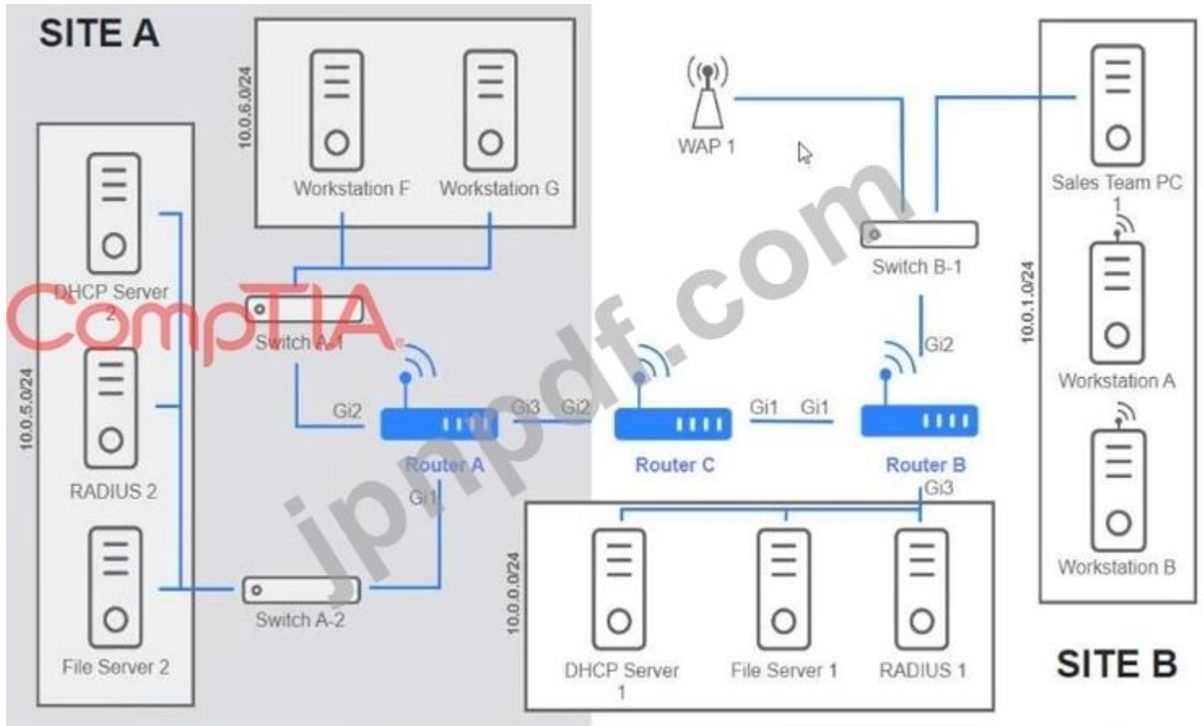
以下の説明のソリューション構成を参照してください。

最新問題: **41**
ログイン情報や属性など、ユーザーに関する機密情報をプロバイダーに渡すことによって機能する XML ベースのセキュリティ概念は次のどれですか。
A. IAM
B. MFA
C. 半径
D. SAML
Answer: (解答を表示する**)**
セキュリティ アサーション マークアップ言語 (SAML) は、特に ID プロバイダー (IdP) とサービス プロバイダー (SP) の間で認証および承認データを交換するために使用される XML ベースの標準です。SAML は、ログイン資格情報や属性などの機密性の高いユーザー情報を ID プロバイダーとサービス プロバイダー間で安全に渡すために、シングル サインオン (SSO) ソリューションでよく使用されます。
* SAML (Security Assertion Markup Language): Web ベースの認証と承認を容易にし、ユーザーが単一の資格情報セットで複数のサービスにアクセスできるようにします。
* XML ベース: XML を使用して認証および承認データをエンコードし、ユーザー情報の安全な送信を保証します。
* アイデンティティ フェデレーション: 異なるセキュリティ ドメイン間でアイデンティティ情報を安全に共有できるため、エンタープライズ SSO ソリューションに最適です。

ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: SAML を含む認証プロトコルについて説明します。
* Cisco Networking Academy: ID 管理とフェデレーション テクノロジーに関するトレーニングを提供します。
* Network+ 認定オールインワン試験ガイド: SAML と、安全な ID 管理および SSO におけるその役割について説明します。

最新問題: **42**
技術者は、企業のサーバーに接続できないユーザーのラップトップのトラブルシューティングを行っています。技術者は、この問題はルーティングに関係していると考えています。技術者は、問題を特定するために次のコマンドのどれを使用する必要がありますか?
A. tcpdump
B. 掘る
C. トレース
D. アルペジオ
Answer: C (メーッセージを残す**)**
tracert (Traceroute) コマンドは、パケットが送信元から送信先までたどるパスを決定するために使用されます。パケットが通過する各ホップと、各ホップにかかる時間を表示することで、ルーティングの問題を特定するのに役立ちます。このコマンドは、接続が失敗している場所や遅延が発生している場所を正確に特定できるため、ルーティングの問題のトラブルシューティングに不可欠なツールです。
参考: CompTIA Network+ の学習教材と一般的なネットワーク トラブルシューティング コマンド。

最新問題: **43**
シミュレーション
ユーザーは、ファイル サーバー 2 にある部門共有のファイルにアクセスできません。ネットワーク管理者は、ワークステーション A とファイル サーバー 2 をホストするネットワーク間のルーティングを検証する役割を担っています。
説明書
各ルータをクリックして出力を確認し、問題を特定し、適切なソリューションを構成します。いつでもトライシミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。



Answer:

以下の説明のソリューション構成を参照してください

Explanation:


Router A
Routing Table
Routing Configuration
CompTIA
Was a problem found?:
Yes
No
Install Static Route
Destination Prefix:
10.0.5.0
Destination Prefix Mask:
255.255.255.0
Interface:
Gi1
Reset to Default
Save
Close

最新問題: **44**
ユーザーは、IP アドレス 10.249.3.76 の内部 Web サイトに接続できません。ネットワーク管理者がコマンドを実行すると、次の出力が表示されます。
1 3ミリ秒 2ミリ秒 3ミリ秒 192.168.25.234
2 2ミリ秒 3ミリ秒 1ミリ秒 192.168.3.100
3 4ミリ秒 5ミリ秒 2ミリ秒 10.249.3.1
4 *
5'
6 *
7 *
ネットワーク管理者は、次のコマンドライン ツールのどれを使用していますか?
A. トレース
B. ネットスタット
C. tcpdump
D. nmap
Answer: (解答を表示する**)**
* Tracert を理解する:
* tracert (Windows では Traceroute) は、パケットが送信元から送信先までたどるパスを追跡するために使用されるコマンドライン ツールです。ルート (各ホップの特定のゲートウェイ) を記録し、IP ネットワーク上のパケットの転送遅延を測定します。

* 出力分析:
* 出力には、一連の IP アドレスと、対応するラウンドトリップ時間 (RTT) がミリ秒単位で表示されます。
* アスタリスク (*) は、それらのホップから応答が受信されなかったことを示します。これは、tracert によって使用される ICMP パケットをブロックするルーターまたはファイアウォールの場合に一般的です。
* 他のツールとの比較:
* netstat: ネットワーク接続、ルーティングテーブル、インターフェース統計などを表示しますが、
* パケットルートをトレースします。
* tcpdump: 分析用にネットワーク パケットをキャプチャし、詳細なネットワーク トラフィックの検査に使用します。
* nmap: パケットルートの追跡ではなく、ネットワーク上のホストとサービスを検出するために使用されるネットワークスキャンツール。
* 使用法：
* tracert は、宛先へのパスを識別し、ネットワーク内の障害点や輻輳点を特定するのに役立ちます。
参考文献:
* ネットワークのトラブルシューティングと診断ツールに関する CompTIA Network+ 学習教材。

最新問題**: 45**
次の攻撃のうち、ネットワーク内で IP アドレスの重複を引き起こす可能性が最も高いのはどれですか?
A. 不正な DHCP サーバー
B. DNS ポイズニング
C. ソーシャルエンジニアリング
D. サービス拒否
Answer: (解答を表示する**)**
* 不正な DHCP サーバーの定義:
* 不正な DHCP サーバーは、ネットワーク上の許可されていない DHCP サーバーであり、適切な制御なしにデバイスに IP アドレスを割り当て、IP アドレスの競合を引き起こす可能性があります。
* 不正な DHCP サーバーの影響:
* IP アドレスの競合: 複数のデバイスが異なる DHCP サーバーから同じ IP アドレスを受信し、ネットワーク接続の問題が発生する可能性があります。
* ネットワークの中断:デバイスに誤ったネットワーク構成設定が割り当てられ、ネットワーク サービスと接続が中断される可能性があります。
* 他の攻撃との比較:
* DNS ポイズニング: DNS レコードを変更してトラフィックを悪意のあるサイトにリダイレクトしますが、IP アドレスの競合は発生しません。
* ソーシャル エンジニアリング: IP アドレスの競合とは直接関係なく、個人を操作して不正アクセスや情報を取得する行為。
* サービス拒否 (DoS): ネットワークまたはサービスに過剰なトラフィックを流して操作を妨害しますが、IP アドレスの重複は発生しません。
* 予防と検出:
* 許可されていないデバイスが DHCP サーバーとして機能するのを防ぐためのネットワーク アクセス制御対策を実装します。
* スイッチで DHCP スヌーピングを使用して、承認された DHCP サーバーからの DHCP 応答のみを許可します。
参考文献:
* ネットワーク セキュリティの脅威と軽減技術に関する CompTIA Network+ 学習教材。

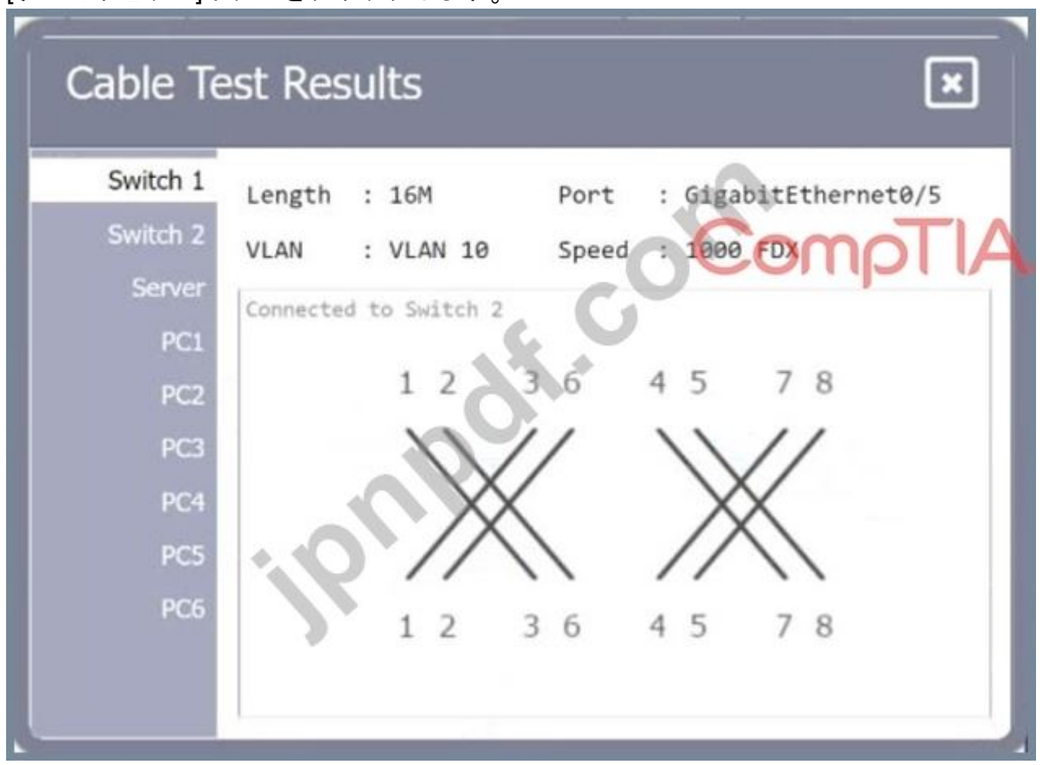
最新問題**: 46**
ネットワーク管理者は、有線デバイスと無線デバイスの両方にアクセスするときに、ユーザーがポートベースの認証フレームワークを使用して企業ネットワークに認証できるようにしたいと考えています。このタスクを実行するのに最適なセキュリティ機能はどれですか。
A. 802.1X

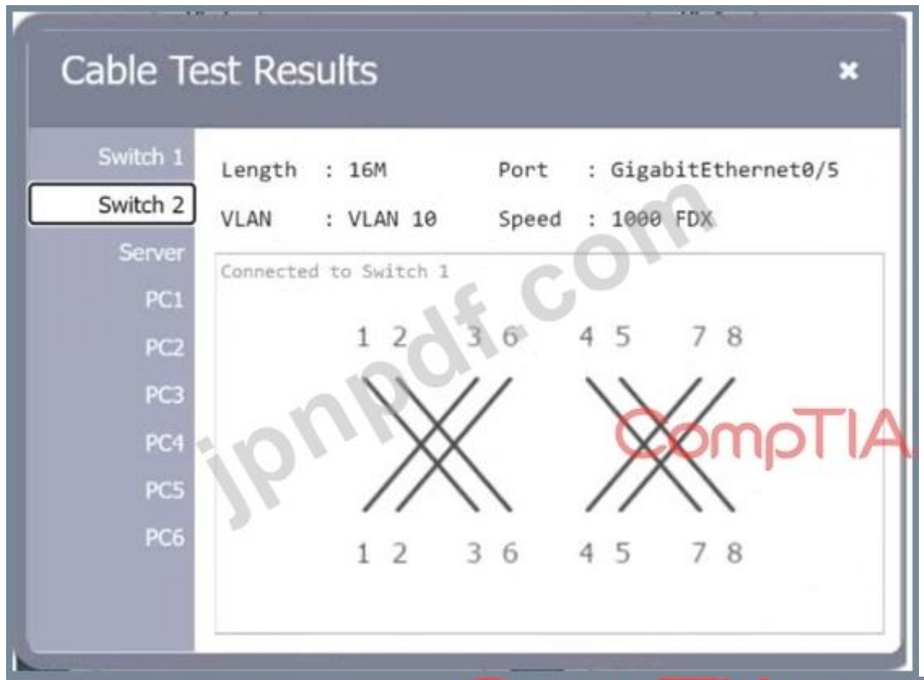
B. アクセス制御リスト
C. ポートセキュリティ
D. MACフィルタリング
Answer: (解答を表示する**)**
802.1X は、LAN または WLAN に接続するデバイスに認証メカニズムを提供するポートベースのネットワーク アクセス制御 (PNAC) プロトコルです。これは、有線または無線のどちらの方法で接続するかに関係なく、認証されたデバイスのみがネットワークにアクセスできるようにする、安全なネットワーク アクセスに広く使用されています。802.1X は、RADIUS などの認証サーバーと連携して、接続しようとしているデバイスの資格情報を検証します。
参考: CompTIA Network+ 学習教材。

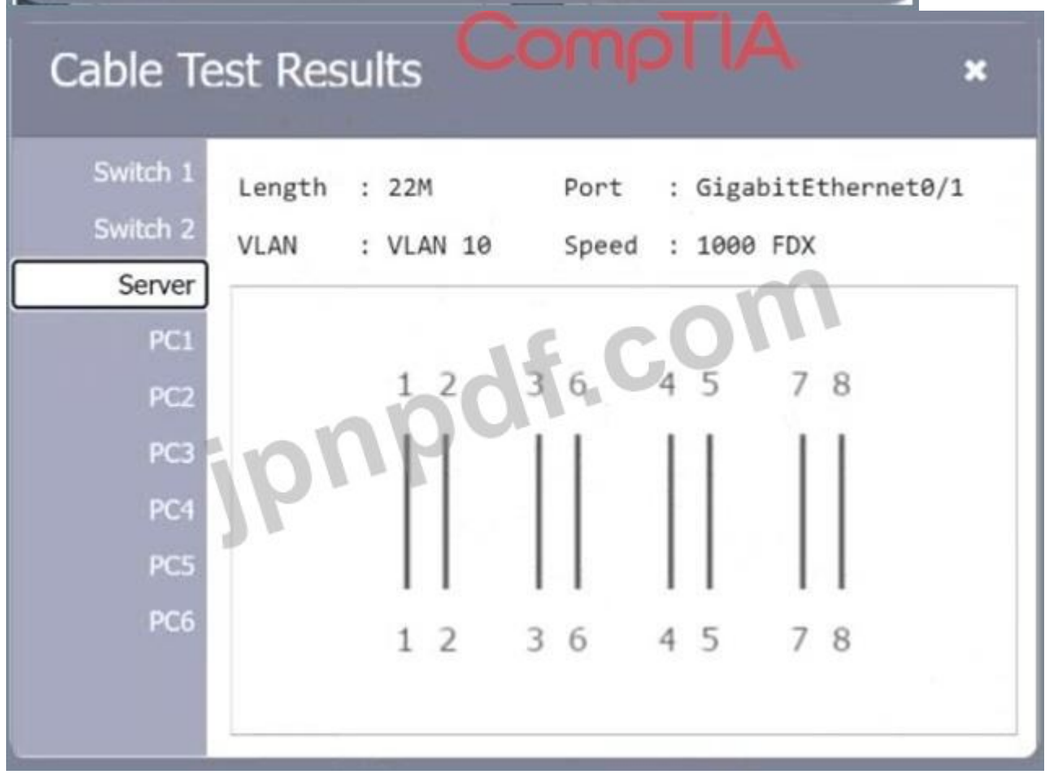
最新問題**: 47**
データ センターの設計者は、一連の Cat 8 キーストーンをインストールした後、テスト中に通常よりも高い干渉に気付きました。設計者は、問題をトラブルシューティングするために、次の手順のどれを実行する必要がありますか。
A. 終端する前に、端部接続が銅テープで巻かれているかどうかを確認します。
B. 従来の圧着プラグの代わりに、パススルー モジュラー圧着プラグを使用します。
C. RX/TX ワイヤを異なるピンに接続します。
D. 100Mbps の速度しか達成できないデバイスで速度テストを実行します。
Answer: A (メーッセージを残す**)**
* 適切な終了の重要性:
* Cat 8 ケーブルでは、信号の整合性を確保し、干渉を減らすために、正確な終端処理が必要です。一般的な要件の 1 つは、シールドを維持し、電磁干渉 (EMI) を減らすために、終端接続を銅テープで包むことです。
* 干渉のトラブルシューティング:
* Cat 8 などの高周波ケーブルの干渉は、不適切なシールドや接地によって発生する可能性があります。端部の接続部が銅テープで適切に巻かれているかどうかを確認することは、重要なステップです。
* 他の選択肢の可能性が低い理由:
* パススルー モジュラー圧着プラグ:干渉の問題とは特に関係がなく、通常はケーブルの組み立てを容易にするために使用されます。
* RX/TX ワイヤを異なるピンに接続すると、干渉が発生するのではなく、接続されないか、データが正しく送信されなくなる可能性があります。
* 100Mbps の速度しか達成できないデバイスで速度テストを実行する: これでは干渉は診断されず、より高速な定格の Cat 8 ケーブルに関する関連情報は提供されません。
* 是正措置:
* 終端処理の前に、すべての端末接続が銅テープで適切に巻かれていることを確認してください。
* 設置全体にわたってシールドが連続しており、適切に接地されていることを確認してください。
* 修正後、ケーブルの干渉を再度テストします。
参考文献:
* CompTIA Network+ の学習教材と構造化ケーブル配線インストール ガイド。

最新問題**: 48**

シミュレーション
ネットワーク技術者は、顧客の SOHO ネットワークに関するいくつかの問題を解決する必要があります。顧客は、一部の PC がネットワークに接続されていないが、他の PC は正常に動作しているようだと報告しています。
説明書
すべてのネットワーク コンポーネントのトラブルシューティングを行います。
まずケーブル テストの結果を確認し、適切な PC、サーバー、およびレイヤー 2 スイッチをクリックして診断します。
問題のあるコンポーネントを特定し、それぞれの問題を修正するための解決策を提案します。
いつでも持ち帰りたい場合は
シミュレーションの初期状態を教えてください
[すべてリセット]ボタンをクリックします。





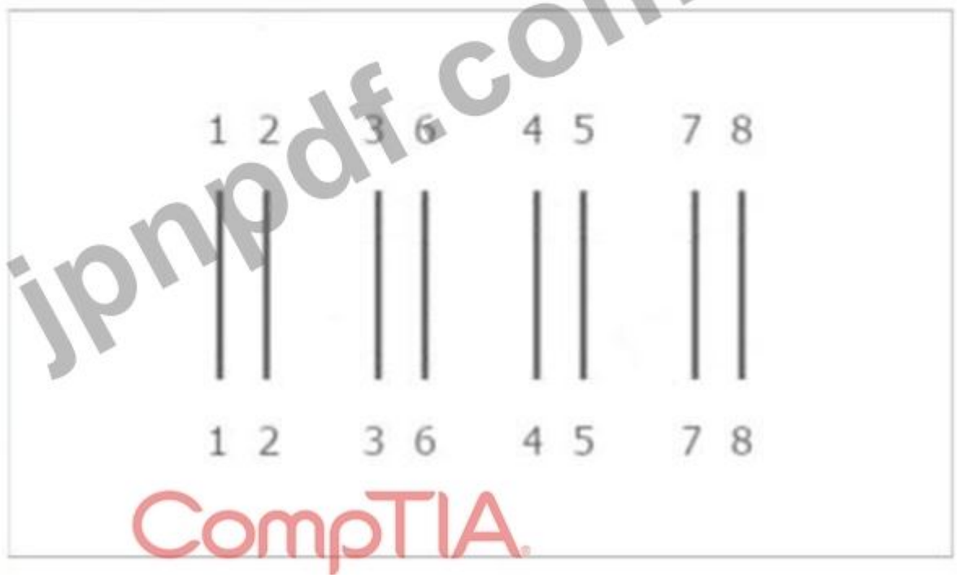


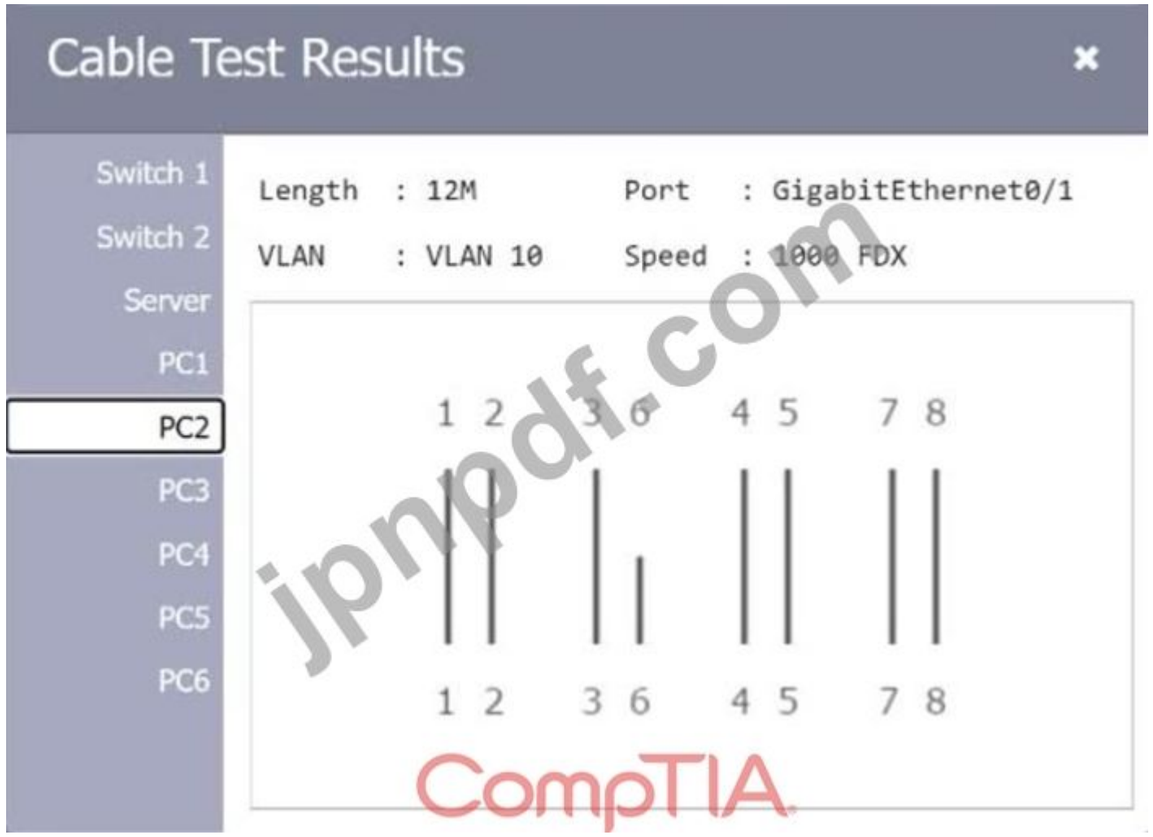
Cable Test Results

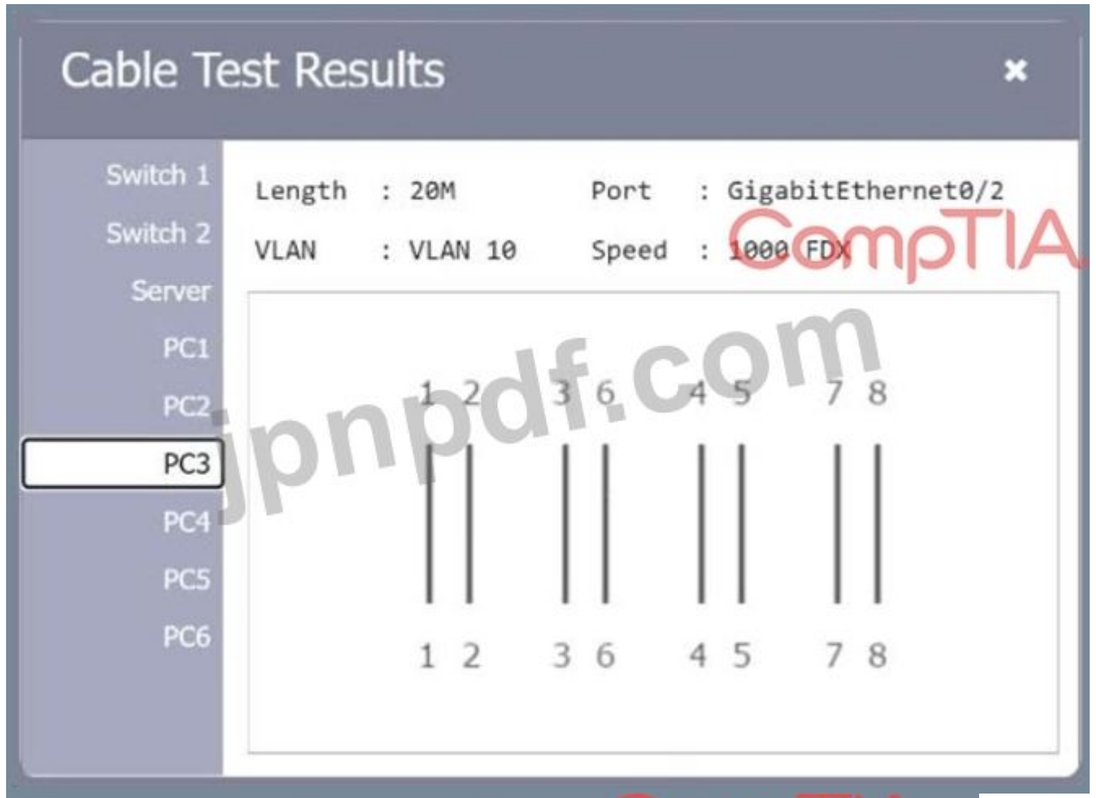
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6

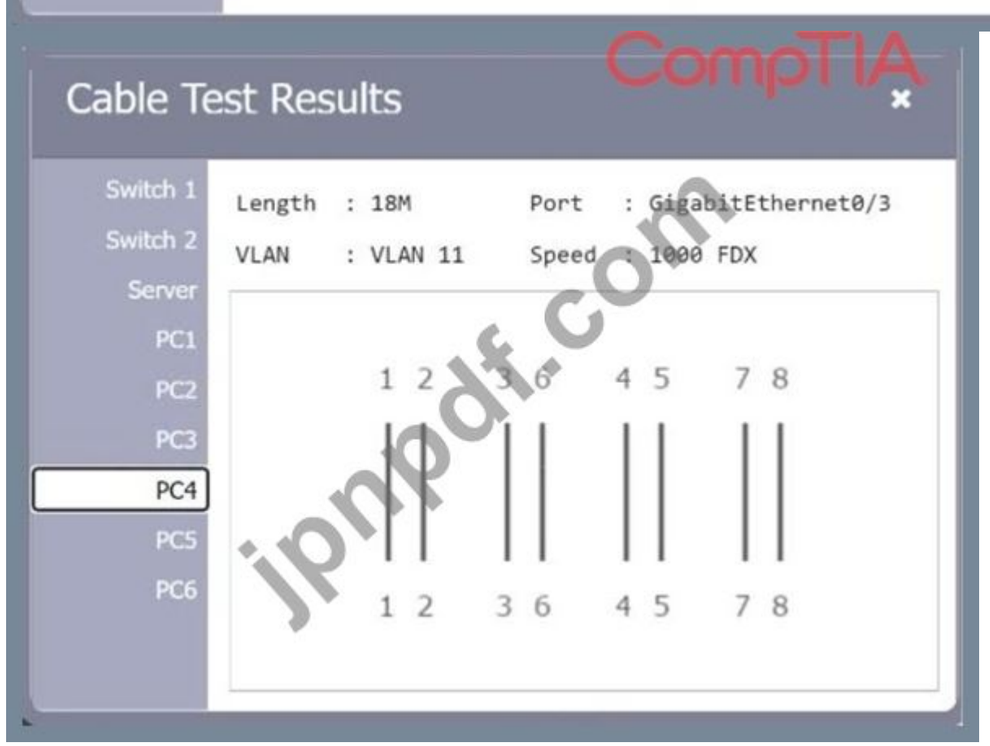
Length : 42M Port : GigabitEthernet0/2

VLAN : VLAN 10 Speed : 1000 FDX




Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 12M
Port : GigabitEthernet0/1
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8
jpnpdf.com
CompTIA



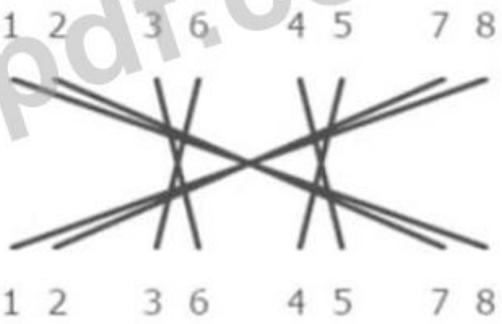


Cable Test Results

Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6

Length : 33M Port : GigabitEthernet0/4

VLAN : VLAN 10 Speed : 1000 FDX

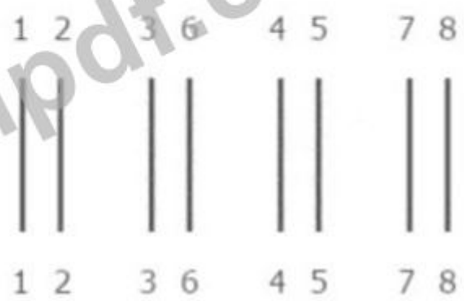


Cable Test Results

Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6

Length : 90M Port : GigabitEthernet0/3

VLAN : VLAN 10 Speed : 1000 FDX

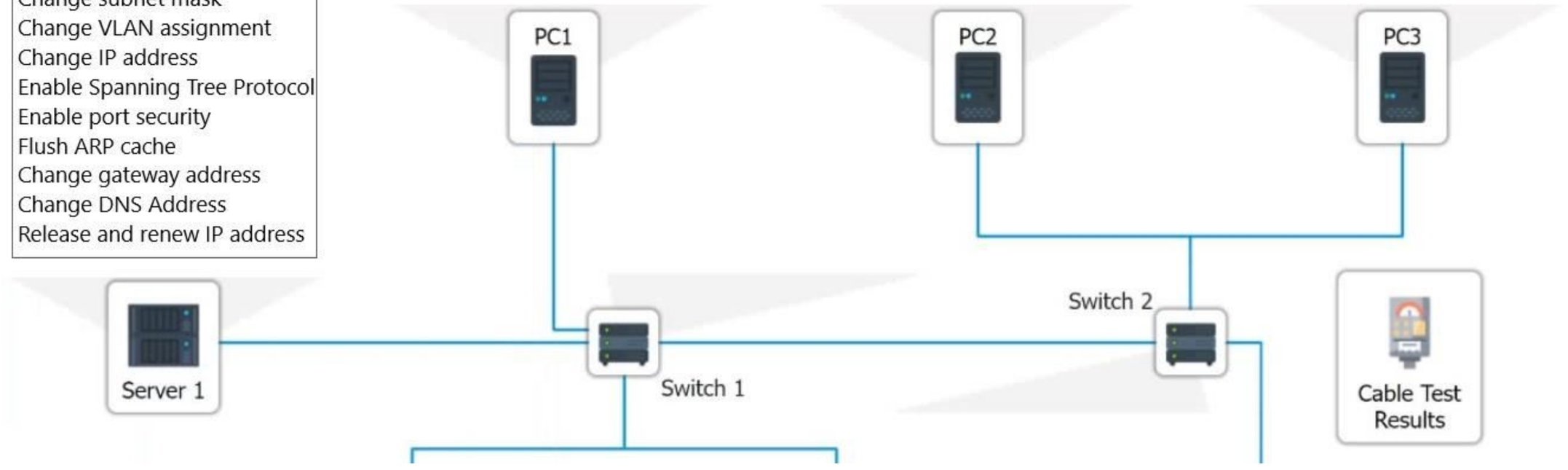


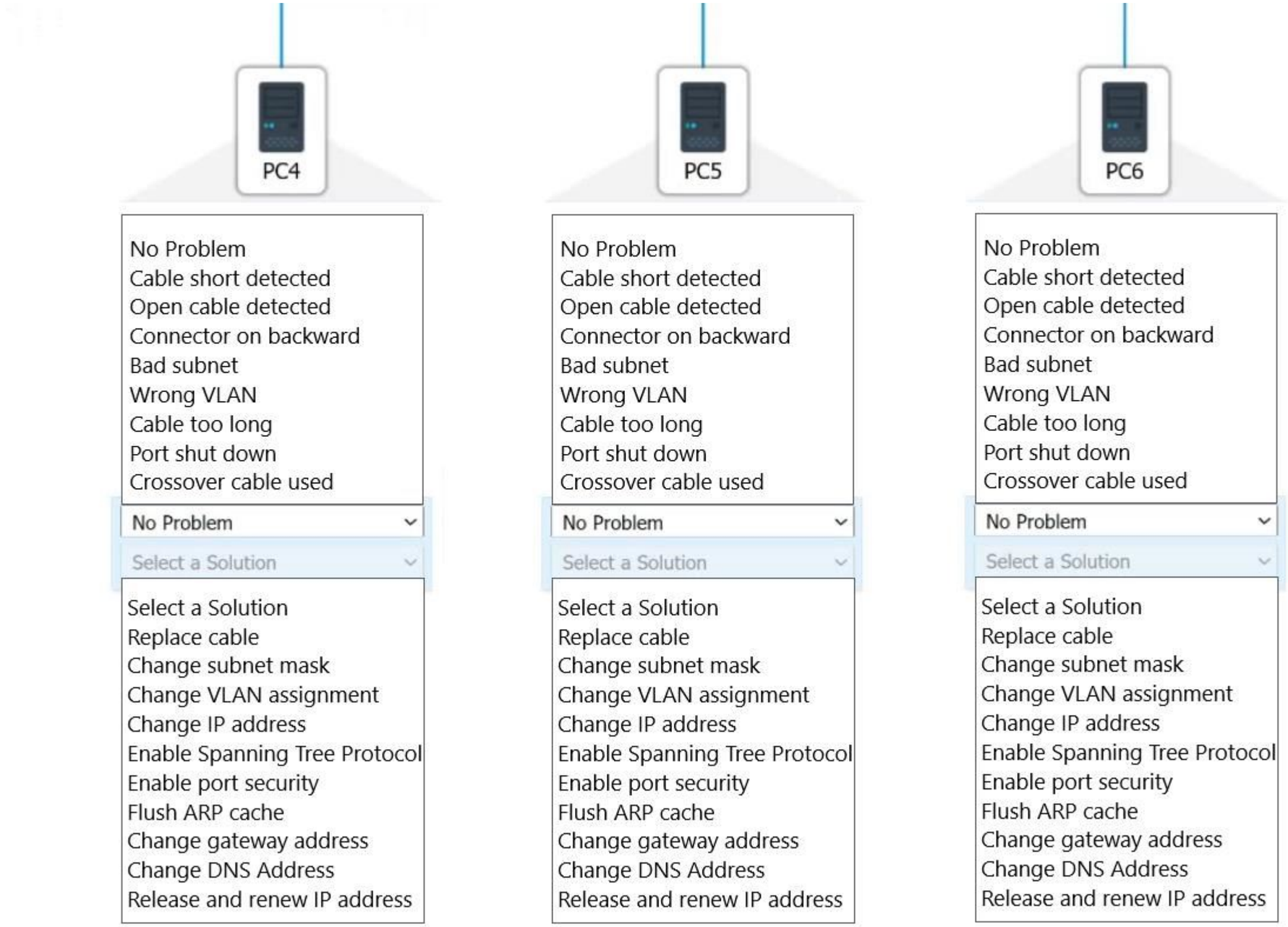
No Problem
Cable short detected
Open cable detected
Connector on backward
Bad subnet
Wrong VLAN
Cable too long
Port shut down
Crossover cable used

No Problem

Select a Solution

Select a Solution
Replace cable
Change subnet mask
Change VLAN assignment
Change IP address
Enable Spanning Tree Protocol
Enable port security
Flush ARP cache
Change gateway address
Change DNS Address
Release and renew IP address

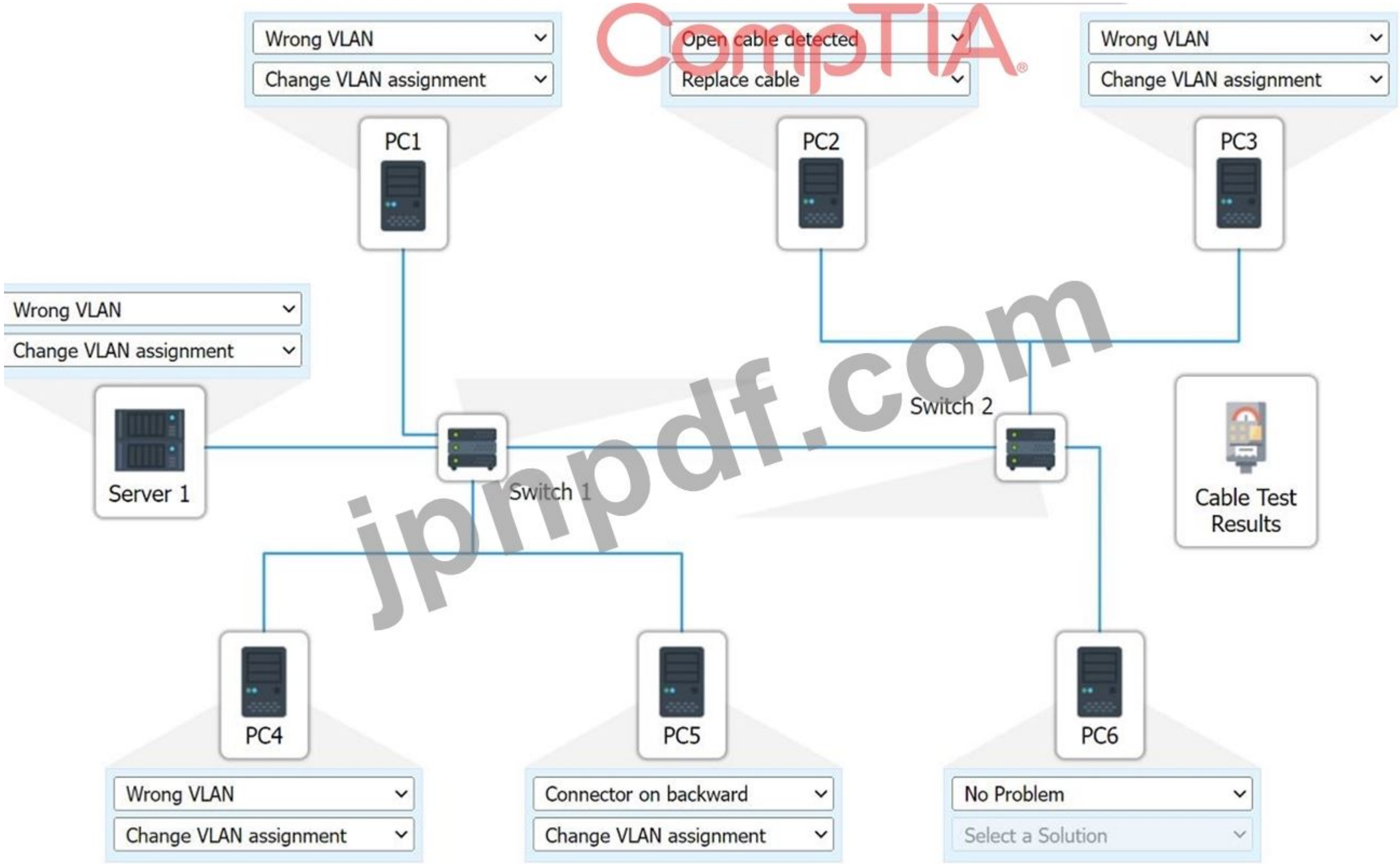




Answer:

答えと解決策は以下をご覧ください

Explanation:



最新問題: **49**

ネットワーク エンジニアは、2 つのサイト間の安全な通信リンクを設計しています。データ ストリーム全体の機密性を維持する必要があります。この目標を達成するには、次のどれが適していますか。

A. GRE
B. IKE
C. 超能力
D. ああ

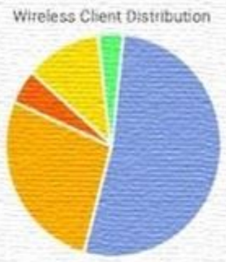
Answer: C (メーッセージを残す)

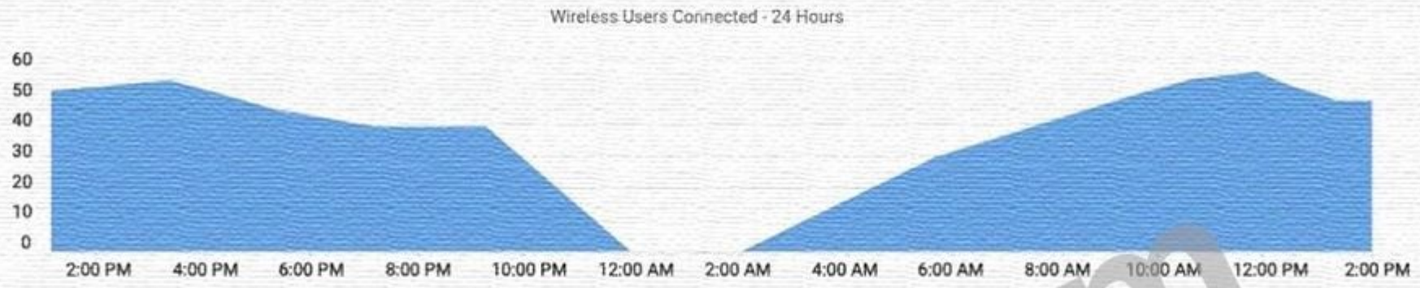
ESP (Encapsulating Security Payload) の定義:
ESP は、ペイロードとオプションの ESP トレーラーを暗号化することでデータの機密性、整合性、信頼性を提供するように設計された IPsec プロトコル スイートの一部です。
機密性の確保:
暗号化: ESP はペイロードを暗号化し、送信中にデータの機密性を保ちます。正しい復号化キーを持つ承認された当事者だけがデータにアクセスできます。
動作モード: ESP は、トランスポート モード (ペイロードのみを暗号化) またはトンネル モード (IP パケット全体を暗号化) で動作できます。どちらも、サイト間のデータを保護するための強力な暗号化を提供します。
他のプロトコルとの比較:
GRE (Generic Routing Encapsulation): 暗号化やセキュリティ機能を提供しないトンネリング プロトコル。
IKE (インターネット キー交換): 安全で認証された通信チャネルを設定するために使用されるプロトコルですが、データ自体は暗号化されません。
AH (認証ヘッダー): IP パケットの整合性と認証を提供しますが、ペイロードは暗号化しません。
実装：
ESP を IPsec VPN 構成の一部として使用して、2 つのサイト間の通信を暗号化し、保護します。これには、IPsec ポリシーを設定し、両方のエンドポイントがデータ暗号化に ESP を使用するように構成されていることを確認することが含まれます。
参照：
IPsec および安全な通信プロトコルに関する CompTIA Network+ 学習教材。

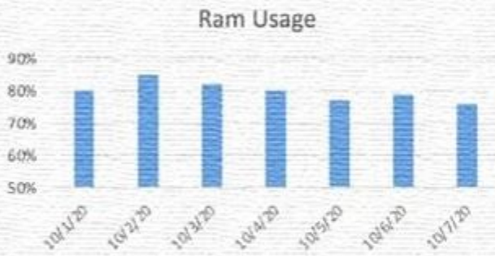
最新問題**: 50**
最近の停電後、アプリケーション サーバーへのアクセスでパフォーマンスの問題がユーザーから報告されています。ワイヤレス ユーザーからも、インターネットが断続的に切断される問題が報告されています。
説明書
画面上部の各タブをクリックします。情報を表示するウィジェットを選択し、ドロップダウン メニューを使用して関連する質問に回答します。いつでもシミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。

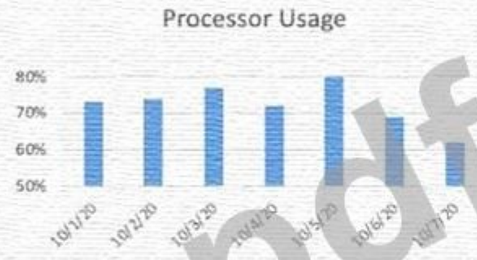
Network Health | Device Monitoring

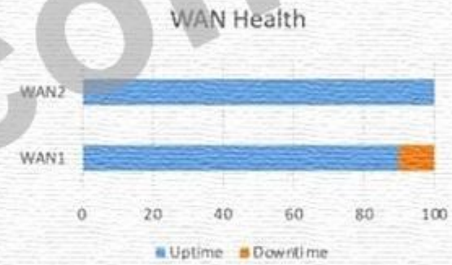
Show Question | Reset All Answers











Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

Which WAN station should be preferred for VoIP traffice?

WAN 1

Select WAN
WAN 1
WAN 2

Network Health | Device Monitoring

Show Question | Reset All Answers

Device Status

Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb

Up (8)

Warning (2)

Down (1)

4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

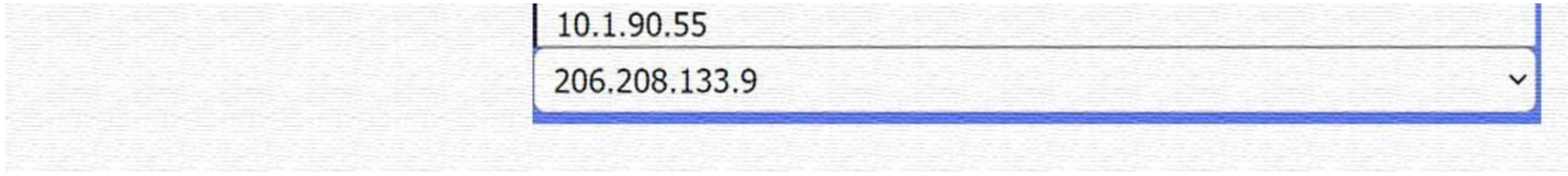
Which device is experiencing connectivity issues?

Select Answer
Router A
Router B
WAP1
WAP2
WirelessController
Switch A
Switch B
DHCP Server
Web Server
APP Server

Router A

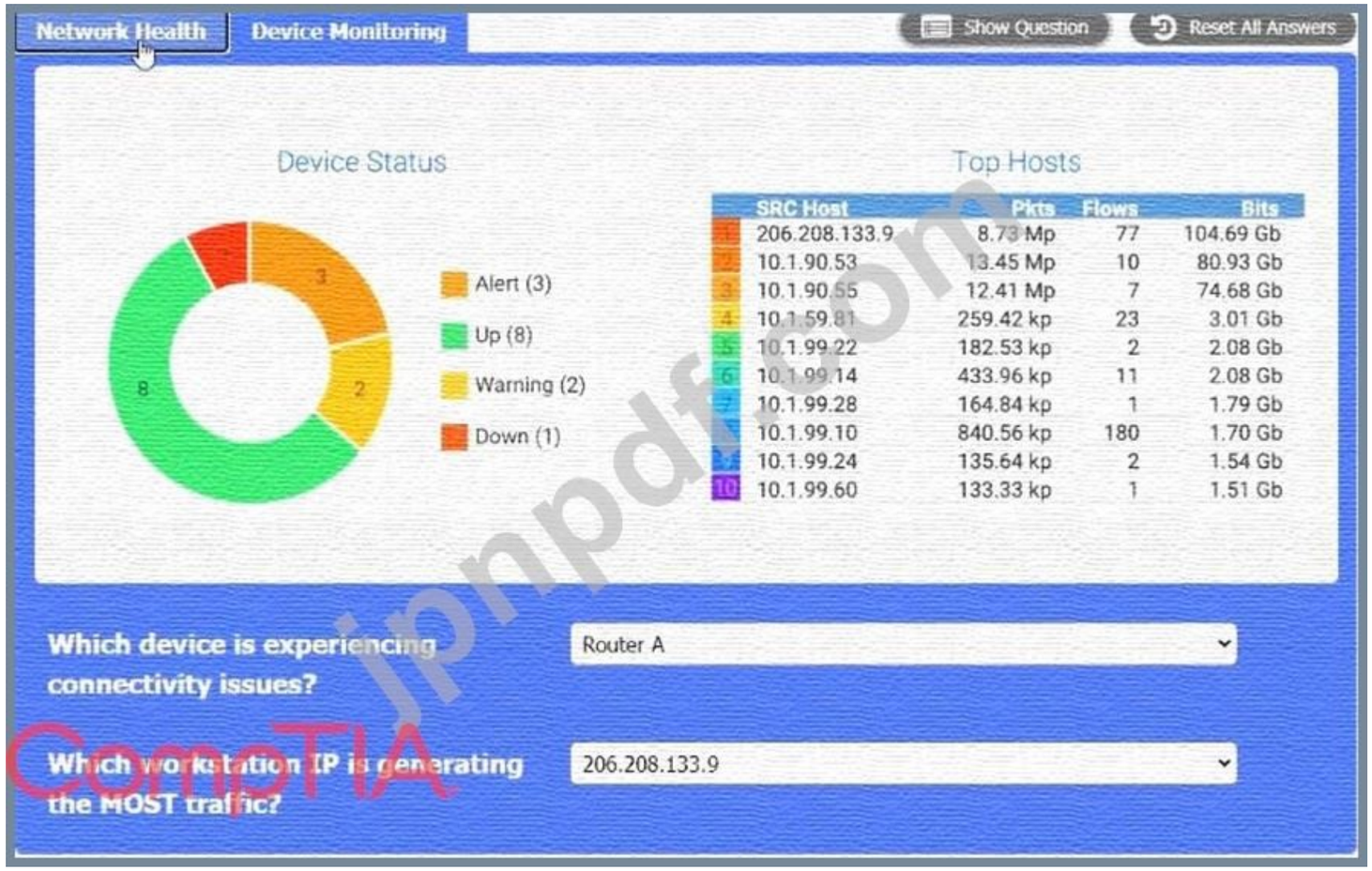
Which workstation IP is generating the MOST traffic?

Select Answer
10.1.99.28
10.1.99.14
10.1.99.10
10.1.99.22
10.1.99.24
206.208.133.10
206.208.133.9
10.1.50.14
10.1.50.13
10.1.59.81
10.1.90.53



Answer:
答えと解決策は下記をご覧ください。
Explanation:
ネットワークの健全性:
WAN 2 は平均遅延と損失率が低いため、VoIP トラフィックに適した WAN ステーションになります。VoIP トラフィックでは、良好な音声品質と信頼性を確保するために、遅延とパケット損失を低く抑える必要があります。WAN 1 は RAM とプロセッサの使用率が高いため、VoIP トラフィックのパフォーマンスにも影響する可能性があります。
提供された画像からの WAN 1 と WAN 2 の主要なメトリックの概要は次のとおりです。
* WAN1:
* アップリンク速度: 10G
* 総使用量: アップロード 26.969GB / ダウン 1.748GB
* 平均スループット: 353MBps アップ / 23.42MBps ダウン
* 損失: 2.51%
* 平均遅延: 24ms
* ジッター: 9.5ms
* WAN 2:
* アップリンク速度: 1G
* 合計使用量: 930GB アップロード / 138GB ダウン
* 平均スループット: 12.21MBps 上り / 1.82MBps 下り
* 損失: 0.01%
* 平均遅延: 11ms
* ジッター: 3.9ms
VoIP トラフィックの場合、音声品質を確保するには、低遅延と低ジッターが特に重要です。WAN 1 は帯域幅とスループットが高いですが、WAN 2 と比較して遅延とジッターも高くなっています。ただし、WAN 2 は損失、遅延、ジッターがはるかに低く、遅延やパケット到着時間の変動に敏感な VoIP トラフィックに適しています。
この情報を考慮すると、WAN 2 は、WAN 1 と比較して帯域幅が低いにもかかわらず、遅延が少なく、ジッタが少なく、損失率が大幅に低いため、VoIP トラフィックに一般的に好まれます。WAN 1 の高帯域幅は、バルク データ転送など、遅延やジッタの影響を受けにくい他の種類のトラフィックに適している可能性があります。

デバイス監視:
接続の問題が発生しているデバイスは、ステータスがダウンしているAPPサーバーまたはルーター1です。
これは、サーバーがネットワーク要求に応答していないか、データを送信していないことを意味します。問題のトラブルシューティングを行うには、APP サーバーの物理的な接続、電源、および構成を確認することをお勧めします。
コンピュータのスクリーンショット 説明は自動的に生成されました



最新問題**: 51**
X.509 証明書が最も一般的に関連付けられているテクノロジは次のどれですか?
A. PKI
B. VLAN タグ付け
C. LDAP
D. MFA
Answer: A (メーッセージを残す**)**
X.509 証明書は、公開キー インフラストラクチャ (PKI) に最もよく関連付けられます。これらの証明書は、デジタル署名、暗号化、認証など、さまざまなセキュリティ機能に使用されます。
* PKI: X.509 証明書は PKI の基本コンポーネントであり、暗号化キーの管理やユーザーとデバイスの認証に使用されます。
* デジタル証明書: Web サイトの SSL/TLS や安全な電子メール通信など、ネットワーク上で安全な通信を確立するために使用されます。
* 認証と暗号化: X.509 証明書は、さまざまなアプリケーションでキーを安全に交換し、ID を検証する手段を提供し、データの整合性と機密性を保証します。
ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: PKI と、ネットワーク セキュリティにおける X.509 証明書の役割について説明します。
* Cisco Networking Academy: PKI、証明書、安全な通信に関するトレーニングを提供します。
* Network+ 認定オールインワン試験ガイド: PKI、X.509 証明書、およびネットワーク通信のセキュリティ保護におけるそれらのアプリケーションについて説明します。
最新問題**: 52**

次の攻撃のうち、企業の Web サイトにアクセスしようとしているユーザーをまったく別の Web サイトに誘導する可能性のあるものはどれですか。
A. DNS ポイズニング
B. サービス拒否
C. ソーシャルエンジニアリング
D. ARPスプーフィング
Answer: (解答を表示する**)**
ネットワーク セグメンテーションでは、ネットワークを小さなセグメントまたはサブネットに分割します。これは、OT (運用技術) デバイスを統合して、これらのデバイスがネットワークの他の部分から分離されるようにする場合に特に重要です。セグメンテーションは、OT デバイスを潜在的な脅威から保護し、セキュリティ インシデントの影響を最小限に抑えるのに役立ちます。また、トラフィックの管理にも役立ち、ネットワーク全体のパフォーマンスを向上させます。
参考: CompTIA Network+ 学習教材。

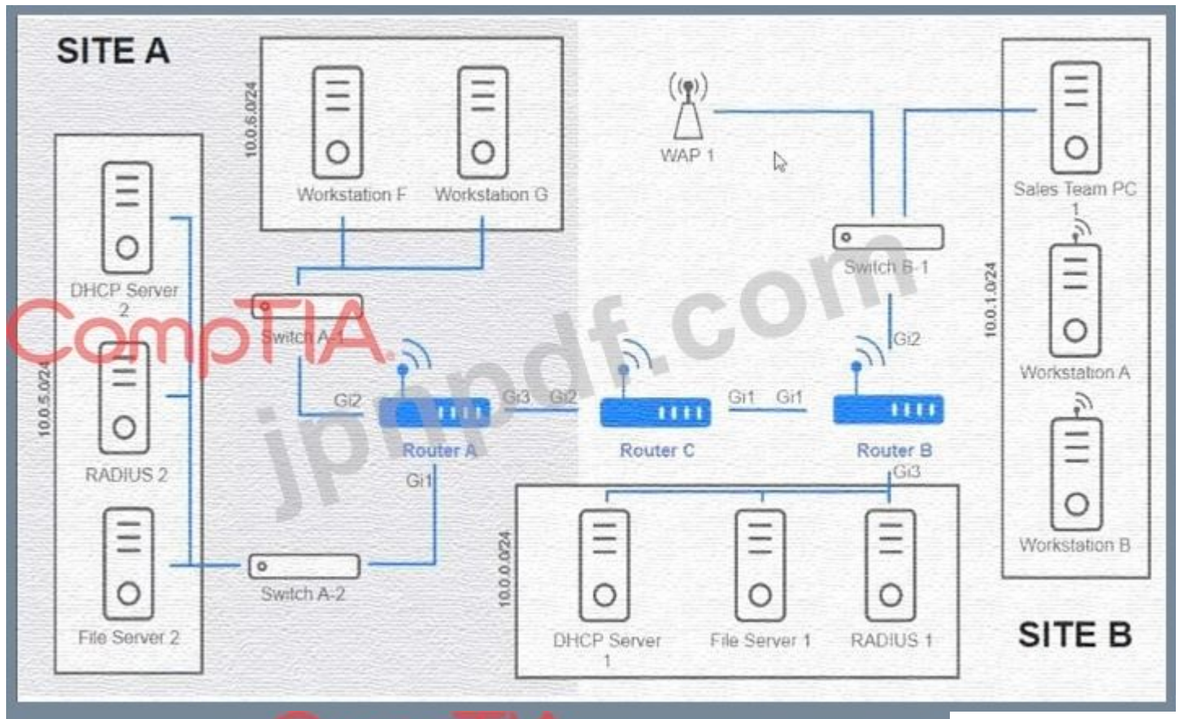
最新問題**: 53**
安全な電子メールに使用されるポートは次のどれですか?
A. 25
B. 110
C. 143
D. 587
Answer: (解答を表示する**)**
ポート 587 は、安全な電子メール送信に使用されます。このポートは、メール クライアントが SMTP プロトコルを使用してメール サーバーにメッセージを送信するために指定されており、通常は暗号化に STARTTLS が使用されます。
* ポート 25: 従来は SMTP リレーに使用されていますが、安全ではなく、スパムの懸念から ISP によって送信メールがブロックされることがよくあります。
* ポート 110: POP3 (Post Office Protocol バージョン 3) に使用されますが、通常はセキュリティ保護されていません。
* ポート 143: IMAP (インターネット メッセージ アクセス プロトコル) に使用され、STARTTLS または SSL/TLS で保護できます。
* ポート 587: 暗号化された認証済み電子メール送信 (SMTP) に特に使用され、クライアントからサーバーへの電子メールの安全な送信を保証します。
ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: 安全な電子メール送信を含む電子メール プロトコルとポートについて説明します。
* Cisco Networking Academy: 電子メール通信のセキュリティ保護と適切なポートの使用に関するトレーニングを提供します。
* Network+ 認定オールインワン試験ガイド: 電子メールのプロトコル、ポート、および電子メール送信のセキュリティ上の考慮事項について説明します。

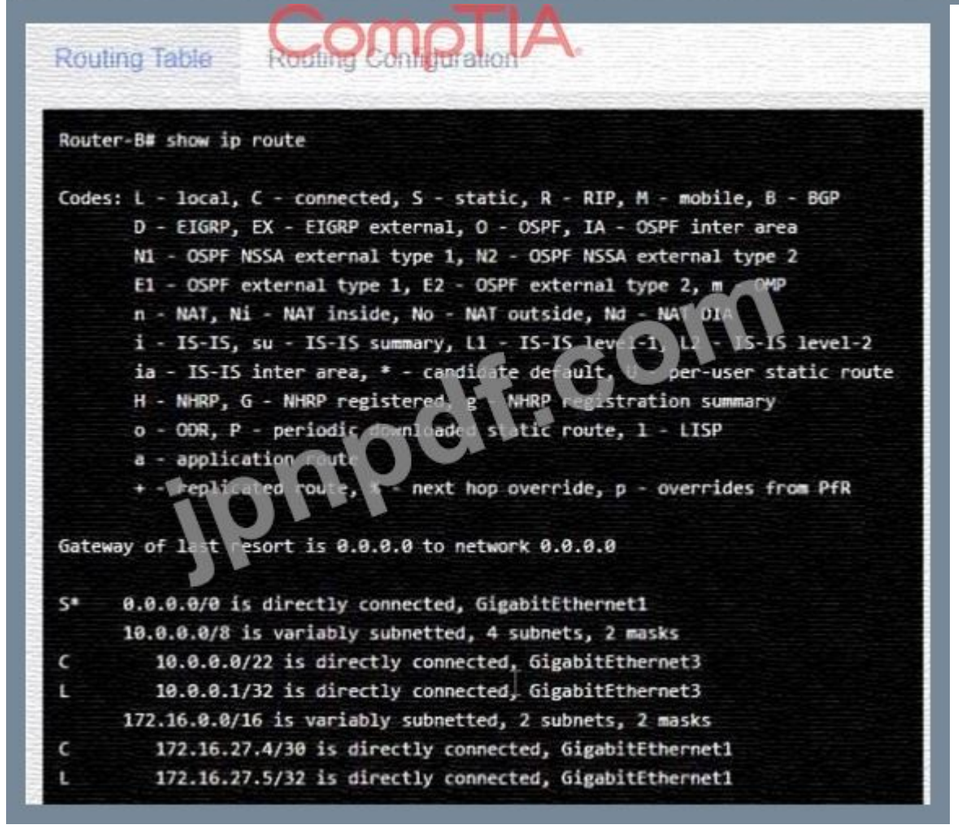
最新問題**: 54**
建物内に機器を設置する際に考慮すべき環境要因は次のどれですか? (2 つ選択してください)。
A. 消火システム
B. UPS の場所
C. 湿度制御
D. 電力負荷
E. 床構造タイプ
F. 最も近いMDFへの近さ
Answer: A (メーッセージを残す**)**
建物内に機器を設置する場合、環境要因は機器の安全性と寿命を確保するために重要です。火災の危険から機器を保護するには、消火システムが不可欠です。湿度制御は、電子部品に悪影響を与える可能性のある腐食やショートなどの湿気関連の損傷を防ぐために不可欠です。両方の要因は、ネットワーク機器に最適な環境を維持するために不可欠です。参考資料:CompTIA Network+ 学習教材。

最新問題: **55**
次の攻撃のうち、企業の Web サイトにアクセスしようとしているユーザーをまったく別の Web サイトに誘導する可能性のあるものはどれですか。
A. DNS ポイズニング
B. サービス拒否
C. ソーシャルエンジニアリング
D. ARPスプーフィング
Answer: A (メーッセージを残す**)**
ネットワーク セグメンテーションでは、ネットワークを小さなセグメントまたはサブネットに分割します。これは、OT (運用技術) デバイスを統合して、これらのデバイスがネットワークの他の部分から分離されるようにする場合に特に重要です。セグメンテーションは、OT デバイスを潜在的な脅威から保護し、セキュリティ インシデントの影響を最小限に抑えるのに役立ちます。また、トラフィックの管理と全体的なネットワーク パフォーマンスの向上にも役立ちます。参考資料:CompTIA Network+ 学習教材。

最新問題: **56**
次のネットワーク トポロジのうち、ネットワーク内のすべてのノード間に直接接続が含まれるのはどれですか。
A. メッシュ
B. ハブアンドスポーク
C. スター
D. ポイントツーポイント
Answer: A (メーッセージを残す**)**
メッシュ トポロジでは、すべてのノードが他のすべてのノードに直接接続されます。これにより、ノード間でデータを移動するためのパスが複数存在するため、高い冗長性と信頼性が実現します。このトポロジは、高可用性が重要なネットワークでよく使用されます。
参考: CompTIA Network+ 学習教材。

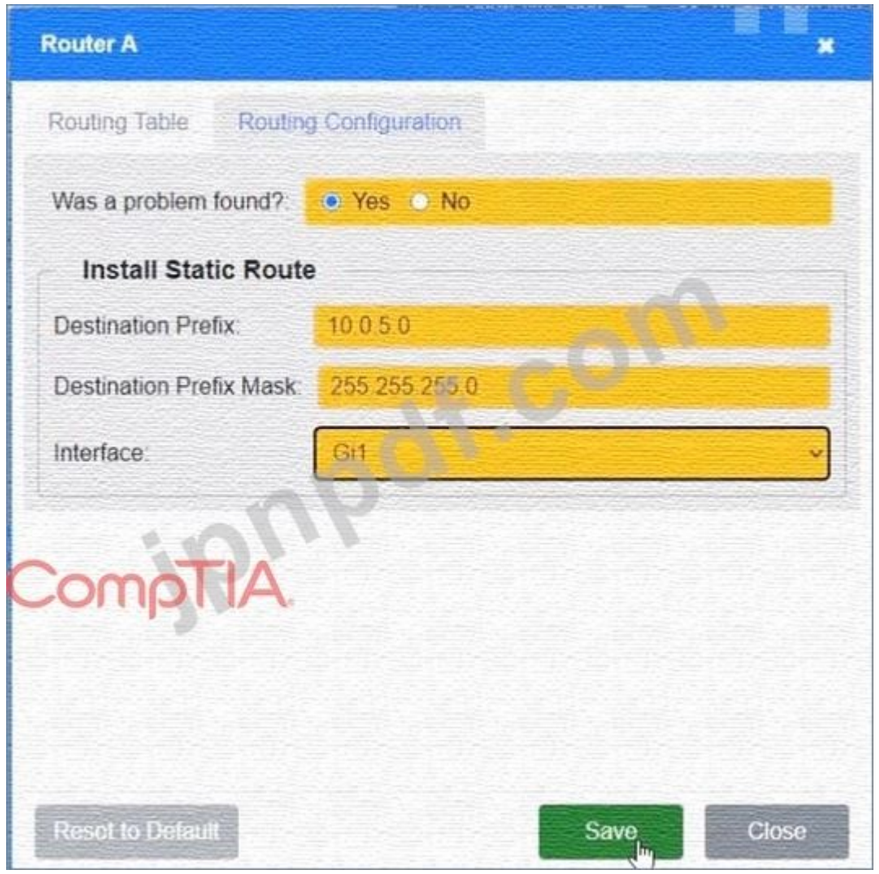
最新問題: **57**
シミュレーション
ユーザーは、ファイル サーバー 2 にある部門共有のファイルにアクセスできません。ネットワーク管理者は、ワークステーション A とファイル サーバー 2 をホストするネットワーク間のルーティングを検証する役割を担っています。
説明書
各ルータをクリックして出力を確認し、問題を特定し、適切なソリューションを構成します。いつでもトライシミュレーションの初期状態に戻したい場合は、[すべてリセット]ボタンをクリックしてください。ルータの図が自動的に生成されます。

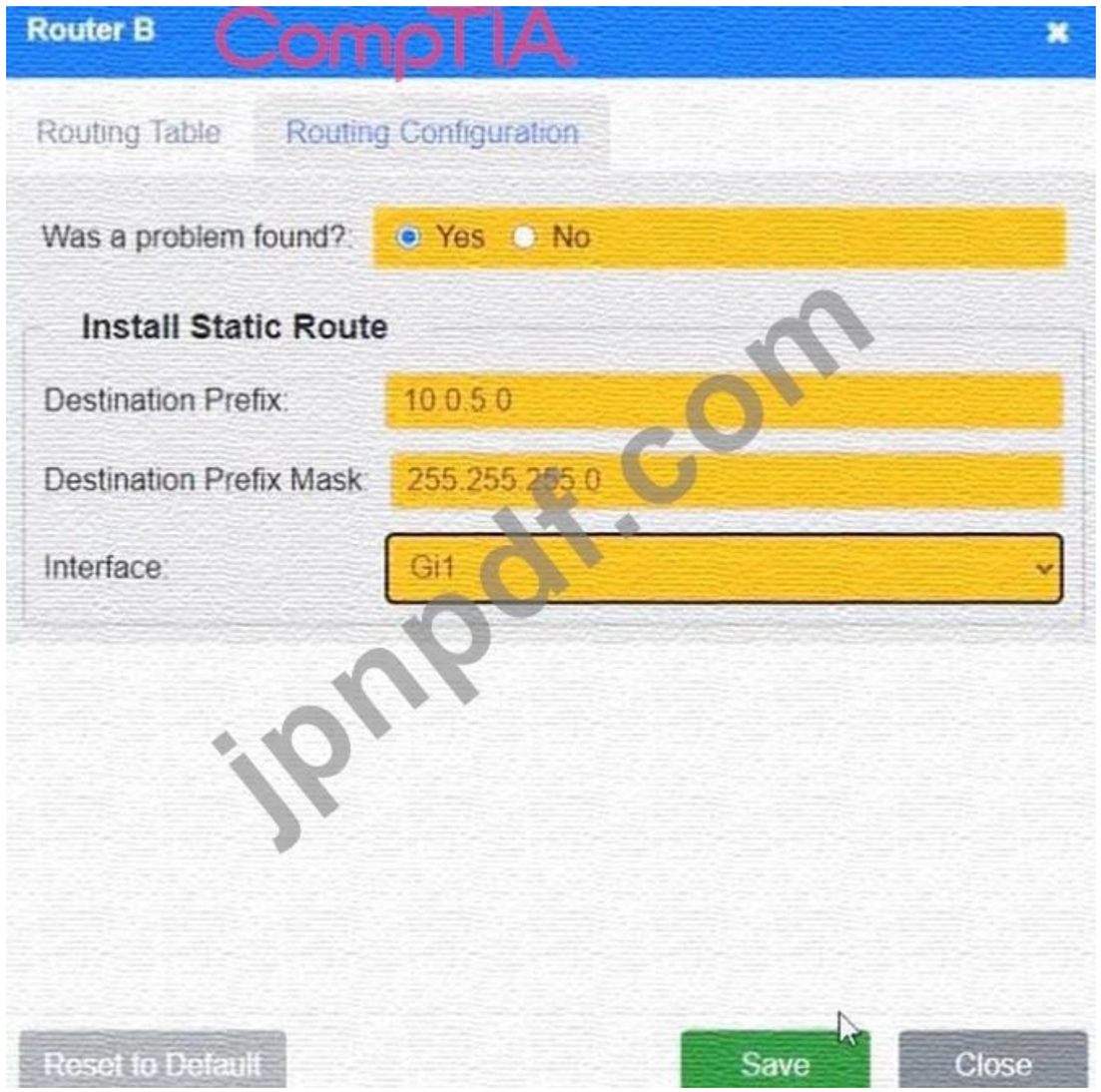




Answer:

以下の説明のソリューション構成を参照してください。


Router A
Routing Table
Routing Configuration
Was a problem found?
Yes
No
Install Static Route
Destination Prefix:
10.0.5.0
Destination Prefix Mask:
255.255.255.0
Interface:
Gi1
Reset to Default
Save
Close


Router B
CompTIA
Routing Table
Routing Configuration
Was a problem found?
Yes
No
Install Static Route
Destination Prefix:
10.0.5.0
Destination Prefix Mask:
255.255.255.0
Interface:
Gi1
Reset to Default
Save
Close

最新問題: **58**
ネットワーク管理者は新しいスイッチを導入しており、スパニング ツリーのデフォルトの優先度値が設定されていることを確認したいと考えています。ネットワーク管理者は次のどの値が表示されると予想しますか。
A. 4096
B. 8192
C. 32768
D. 36684
Answer: C (メーッセージを残す)
* スパニングツリープロトコル (STP)について:
* STP は、一部の冗長パスを選択的にブロックするスパニング ツリーを作成することにより、イーサネット ネットワークでのネットワーク ループを防ぐために使用されます。
* デフォルトの優先度値:
* ブリッジ プライオリティ: STP はブリッジ プライオリティを使用して、どのスイッチがルート ブリッジになるかを決定します。
ほとんどのスイッチのデフォルトのブリッジ優先度値は 32768 です。
* 優先度範囲: ブリッジ優先度は 0 ～ 61440 の範囲で 4096 単位で設定できます。
* 構成と検証:
* 新しいスイッチを導入する場合、ネットワーク管理者は show spanning-tree などのコマンドを使用してブリッジの優先順位を確認し、それがデフォルト値の 32768 に設定されているかどうかを確認できます。
* 他の値との比較:
* 4096 および 8192: デフォルトの優先度よりも低いため、手動で優先度を高く設定する必要があることを示します。

* 36684: 非標準の値。特定の構成変更の結果である可能性があります。
参考文献:
* スパニング ツリー プロトコルとネットワーク構成に関する CompTIA Network+ 学習教材。

最新問題**: 59**
ネットワーク管理者は新しいスイッチを構成しており、割り当てられたデバイスのみがスイッチに接続できるようにしたいと考えています。管理者は次のどれを行う必要がありますか?
A. ポートセキュリティを有効にします。
B. 不要なサービスを無効にします。
C. ACL を設定します。
D. キャプティブポータルを実装します。
Answer: A (メーッセージを残す**)**

最新問題**: 60**
ネットワーク技術者は、新しく入居したオフィスのアクセス スイッチに UTP パッチ パネルからパッチ コードを取り付ける必要があります。パッチ パネルには、ジャックを簡単に識別できるようにラベルが付いていません。適切なパッチ パネル ポートを識別する最も簡単な方法は、次のどのツールですか。
A. トナー
B. ラップトップ
C. ケーブルテスター
D. 視覚的障害検出装置
Answer: (解答を表示する**)**
トナー プローブ (トナーおよびプローブ キットとも呼ばれる) は、特にパッチ パネルにラベルが付いていない場合に、束の中の個々のケーブルを識別するための最も簡単で効果的なツールです。トナーはケーブルを通じて可聴音を送信し、プローブは反対側でその音を検出します。これにより、技術者は正しいケーブルをすばやく識別できます。
* 機能: トナーはケーブルに沿って伝わる音を生成します。プローブを正しいケーブルの近くに置くと、音が検出され、音が発せられます。
* 使いやすさ: トナープローブは、ケーブルが多い環境でも簡単に使用できるため、
* ラベルのないパッチ パネル内のケーブルを識別するのに最適です。
* 効率: この方法は、特に複雑な設定の場合、手動でトレースするよりもはるかに高速で信頼性が高くなります。
ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: ケーブルの識別とトラブルシューティングに使用されるツールの詳細を説明します。
* Cisco Networking Academy: トナー プローブやその他のケーブル テスト ツールの使用方法に関するトレーニングを提供します。
* Network+ 認定オールインワン試験ガイド: ネットワーク ケーブルの識別と管理のためのさまざまなツールの使用について説明します。

最新問題**: 61**
スプリット トンネル VPN のコスト効率の面での利点は次のどれですか。
A. Web トラフィックは Web フィルターによってフィルター処理されます。
B. 会社のインターネット接続には、より多くの帯域幅が必要です。
C. 監視により、会社のネットワーク上の安全でないマシンが検出されます。
D. クラウドベースのトラフィックは会社のネットワーク外に流れます。
Answer: D (メーッセージを残す**)**
スプリット トンネル VPN を使用すると、特定のトラフィック (クラウドベースのサービスなど) が VPN をバイパスしてインターネットに直接アクセスできます。これにより、会社の VPN とインターネット接続を通過するトラフィックの量が減り、帯域幅が節約され、コストが削減されます。また、すべてのトラフィックが同じレベルの検査やフィルタリングの対象となるわけではないため、クラウド

ベースのサービスのパフォーマンスが向上します。
参考: CompTIA Network+ 学習教材。

最新問題: **62**
会社の会計担当者が財務部門の共有フォルダしか閲覧できない場合、会社が実施する可能性が高いのは次のどれですか。
A. 一般データ保護規則
B. 最小権限のネットワークアクセス
C. 利用規定
D. エンドユーザー使用許諾契約
Answer: B (メーッセージを残す**)**
最小権限ネットワーク アクセスは、ユーザーのアクセス権を、職務を遂行するために必要なものだけに制限する原則です。この場合、会計士のアクセスは財務部門の共有フォルダーのみに制限され、ネットワークの他の部分に不必要にアクセスできないようにします。これにより、不正アクセスや潜在的なデータ侵害のリスクが軽減されます。参考資料: CompTIA Network+ 試験目標および公式学習ガイド。

最新問題: **63**
サポート担当者は、リモートユーザーの有線デバイスが頻繁に切断され、速度が遅いという報告を受けました。調査の結果、サポート担当者はユーザーの同軸モデムの信号電力が -97dB。
A. ラインに接続されているスプリッターを削除する
B. デバイスをワイヤレスに切り替える
C. デバイスを現代のものに近づける
D. ネットワーク速度を下げる
Answer: A (メーッセージを残す**)**
信号強度が -97dB の場合、信号が非常に弱いことを示し、接続の問題や速度低下の原因となる可能性があります。
同軸回線上のスプリッターは信号品質をさらに低下させる可能性があるため、スプリッターを取り外すと信号強度と全体的な接続品質が向上します。
* 信号品質: スプリッターは信号を複数の回線に分割することで信号強度を低下させる可能性がありますが、信号がすでに弱い場合は悪影響を与える可能性があります。
* 直接接続: モデムから着信回線への直接接続を確保することで、信号品質を最大限に高め、潜在的な障害点を減らすことができます。
ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: 接続の問題のトラブルシューティングと信号強度がネットワーク パフォーマンスに与える影響について説明します。
* Cisco Networking Academy: ネットワーク設定で最適な信号品質を維持するための洞察を提供します。
* Network+ 認定オールインワン試験ガイド: 信号劣化に関連する問題やその軽減方法など、一般的なネットワークの問題について説明します。

最新問題: **64**
管理者は、企業ネットワークで使用するために SNMP サーバーをセットアップしており、MIB 内にデバイス ID を作成する必要があります。MIB の機能について説明しているのは次のどれですか。
A. DHCPリレーデバイス

B. ポリシー適用ポイント
C. イベント変換の定義ファイル
D. ネットワーク アクセス コントローラ
Answer: (解答を表示する**)**
* MIB (管理情報ベース): MIB は、通信ネットワーク内のエンティティを管理するために使用されるデータベースです。MIB は、簡易ネットワーク管理プロトコル (SNMP) によってイベントを読み取り可能な形式に変換するために使用され、ネットワーク管理者がネットワーク デバイスを効果的に管理および監視できるようにします。
* MIB の機能: MIB には、SNMP を使用してネットワーク上で管理できるすべてのオブジェクトの定義と情報が含まれています。これらのオブジェクトは、オブジェクト識別子 (OID) を含む階層型の名前空間を使用して定義されます。

最新問題**: 65**
VoIP 電話がポートに接続されていますが、通話を受信できません。この問題を解決するには、ポートで次のどれを実行する必要がありますか?
A. ポート上のすべての VLAN をトランクします。
B. ネイティブVLANを設定します。
C. トラフィックを音声 VLAN にタグ付けします。
D. VLAN を無効にします。
Answer: (解答を表示する**)**
* VoIP と VLAN について理解する:
* VoIP (Voice over IP) 電話では、パフォーマンスとセキュリティを向上させるために、音声トラフィックをデータ トラフィックから分離するために、VLAN (仮想ローカル エリア ネットワーク) がよく使用されます。
* 音声VLANへのトラフィックのタグ付け:
* 音声 VLAN 構成: スイッチのポートは、特定の音声 VLAN のトラフィックにタグを付けるように構成する必要があります。これにより、音声パケットが優先され、正しく処理されるようになります。
* VLAN タグ付け:VLAN タグ付けにより、スイッチはネットワーク上の音声トラフィックを他の種類のトラフィックから識別して分離できるため、VoIP 通信の遅延とジッターが削減されます。
* 他のオプションとの比較:
* ポート上のすべての VLAN をトランキングする: すべての VLAN のトランキングは、通常、個々のデバイス ポートではなく、スイッチ間のリンクに使用されます。
* ネイティブ VLAN を設定します。ネイティブ VLAN はタグなしトラフィック用であり、音声トラフィックを分離して優先順位を付ける必要性には対応していません。
* VLAN を無効にする:VLAN を無効にすると、音声トラフィックとデータ トラフィックが混在し、パフォーマンスの問題が発生したり、トラフィックが分離されなかったりする可能性があります。
* 実装：
* VoIP 電話に接続されたスイッチ ポートを設定して、指定された音声 VLAN のトラフィックにタグを付け、適切なネットワーク セグメンテーションとサービス品質を確保します。
参考文献:
* VLAN 構成と VoIP 実装に関する CompTIA Network+ 学習教材。

最新問題**: 66**
重要なインフラストラクチャ スイッチのサポートが終了していると判断されました。セキュリティを確保するための最適な次のステップは次のうちどれですか。
A. 最新のパッチとバグ修正を適用します。
B. スイッチを廃止して交換します。
C. 現在のファームウェアに問題がないことを確認します。
D. スイッチをネットワークから分離します。
Answer: B (メーッセージを残す**)**
サポート終了について理解する:
サポート終了ステータス: ベンダーがデバイスのサポート終了を宣言すると、そのデバイスは更新、パッチ、またはテクニカル サポートを受けられなくなります。新しい脆弱性が解決されないため、セ

キュリティ リスクが生じます。
サポートが終了したデバイスを保持することのリスク:
セキュリティの脆弱性: 更新を行わないと、スイッチは新たなセキュリティの脅威にさらされることになります。
コンプライアンスの問題: 多くの規制フレームワークでは、重要なインフラストラクチャをサポートされた安全なハードウェアで維持することが求められています。
最善の次のステップ - 交換:
廃止と交換: 最も安全な方法は、サポートが終了したスイッチを新しいサポート対象モデルに交換することです。これにより、インフラストラクチャが安全で、現在の標準に準拠した状態が維持されます。
計画と実行: ネットワークのニーズを評価し、適切な交換スイッチを選択し、ハードウェア交換のためのダウンタイムをスケジュールすることで、交換を計画します。
他のオプションとの比較:
最新のパッチを適用する: これは役に立ちますが、今後パッチが提供されないため、将来の脆弱性には対処できません。
現在のファームウェアに問題がないことを確認する: これは一時的な対策に過ぎず、将来のリスクを軽減するものではありません。
スイッチをネットワークから分離する: スイッチを分離すると、ネットワークの動作が中断される可能性があり、長期的な解決策としては実行可能ではありません。
参照：
ネットワークメンテナンスとセキュリティのベストプラクティスに関する CompTIA Network+ 学習教材。

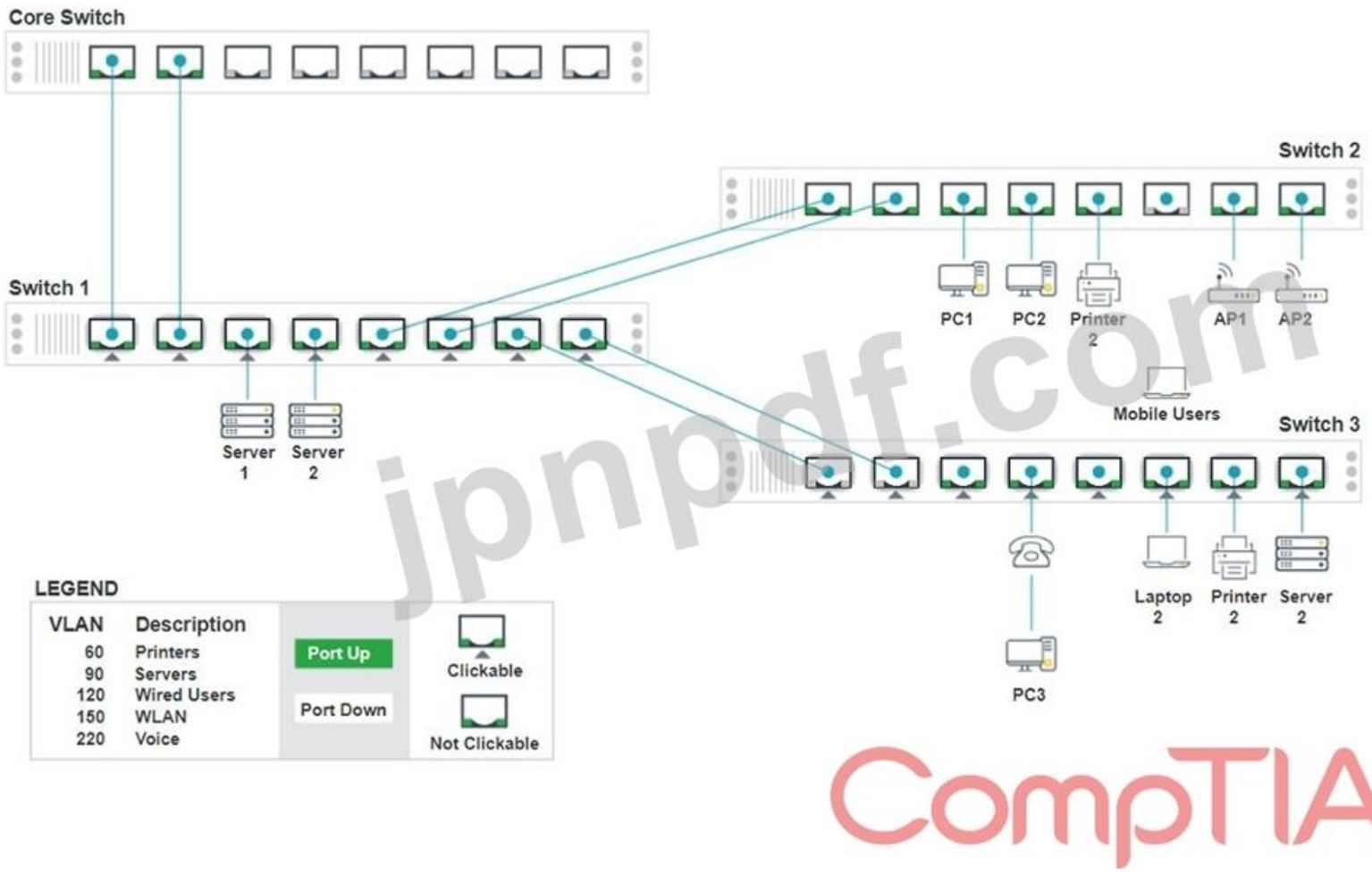
最新問題**: 67**
ネットワーク管理者は、ネットワーク内の 2 つのレイヤー 2 スイッチを接続しています。これらのスイッチは、複数のネットワークでデータを転送する必要があります。この要件を満たすのは次のどれですか。
A. ジャンボフレーム
B. 802.1Q タグ付け
C. ネイティブVLAN
D. リンクアグリゲーション
Answer: (解答を表示する**)**
802.1Q タグ付け (VLAN タグ付けとも呼ばれる) は、スイッチ間のトランク リンク上の VLAN を識別するために使用されます。これにより、スイッチは単一の物理接続を介して複数の VLAN (またはネットワーク) のデータを転送できます。この方法により、異なる VLAN からのトラフィックがネットワーク全体で適切に分離され、管理されます。
参考: CompTIA Network+ 学習教材。

最新問題**: 68**
ネットワーク管理者のデバイスは、企業本社内で深刻な Wi-Fi 干渉を受けており、デバイスが頻繁にネットワークから切断される状態になっています。この問題の原因として最も可能性が高いのは次のどれですか。
A. クライアント接続が多すぎます
B. 無線吸収が多すぎる
C. 無線リピーターが多すぎます
D. 無線反射が多すぎる
Answer: D (メーッセージを残す**)**

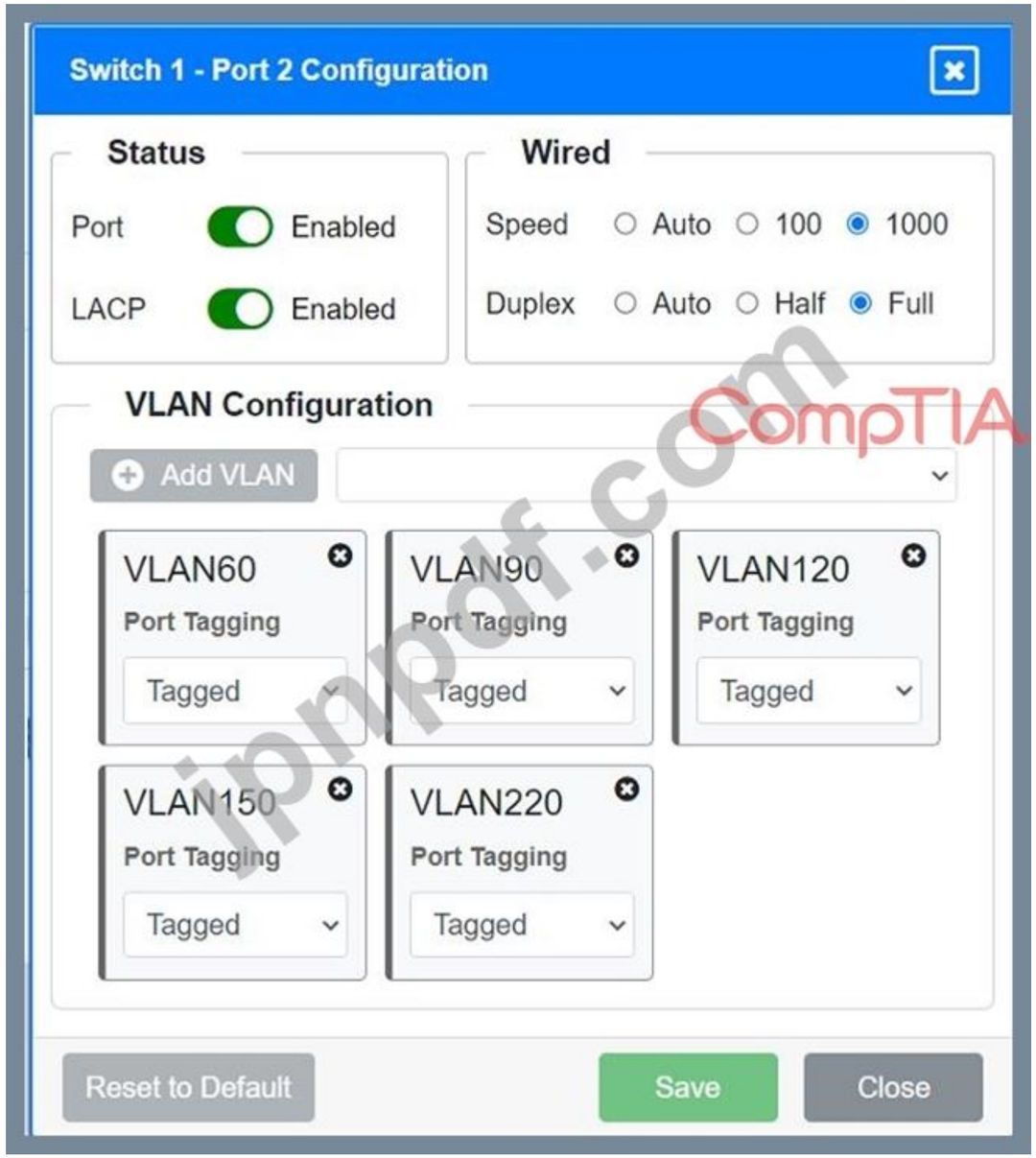
最新問題**: 69**
ネットワーク管理者は、ルーターのインターフェイスを 10.0.0.95 255.255.255.240 に設定しました。管理者は、ルーターが IP 10.0.0.81/28 の Web サーバーにパケットをルーティングしていないことを発見しました。次のどれが最適な説明ですか?
A. Web サーバーは別のサブネットにあります。

B. ルータインターフェースはブロードキャストアドレスです。
C. IP アドレス空間はクラス A ネットワークです。
D. サブネットはプライベート アドレス空間内にあります。
Answer: B (メーッセージを残す)
* サブネット化の理解:
* サブネット マスク 255.255.255.240 (または /28) は、各サブネットに 16 個の IP アドレス (使用可能なアドレス 14 個、ネットワーク アドレス 1 個、ブロードキャスト アドレス 1 個) があることを示します。
* サブネット範囲の計算:
* サブネット計算: /28 サブネット マスクを持つ IP アドレス 10.0.0.95 の場合:
* ネットワークアドレス: 10.0.0.80
* 使用可能なIP範囲: 10.0.0.81〜10.0.0.94
* ブロードキャストアドレス: 10.0.0.95
* ルーターインターフェース構成:
* ブロードキャストアドレスの問題:IPアドレス10.0.0.95はサブネットのブロードキャストアドレスです
10.0.0.80/28。ブロードキャスト アドレスを使用してルーター インターフェイスを構成すると、有効なホスト アドレスではないため、ルーティングの問題が発生します。
* 他のオプションとの比較:
* Web サーバーは異なるサブネットにあります:Web サーバー (10.0.0.81) は同じサブネット範囲 (10.0.0.80/28) 内にあります。
* IP アドレス空間はクラス A ネットワークです: 10.0.0.0 はクラス A ネットワークですが、ブロードキャスト アドレスによって発生するルーティングの問題は説明されません。
* サブネットはプライベート アドレス空間内にあります:プライベート アドレス空間の指定 (RFC 1918) は、ブロードキャスト アドレス構成に関連するルーティングの問題には影響しません。
* 解決：
* 使用可能な範囲内の有効なホストIPアドレスを使用してルータインターフェイスを再設定します。
10.0.0.94。
参考文献:
* サブネットと IP アドレス構成に関する CompTIA Network+ 学習教材。

最新問題**: 70**
シミュレーション
ネットワーク技術者がアクセス レイヤー スイッチを交換し、接続されたデバイスが正しいネットワークに接続できるように再構成する必要があります。
説明書
スイッチ 1 とスイッチ 3 の適切なポートをクリックして、正しい設定を確認または再構成します。
* 各デバイスが特定のデバイスのみにアクセスできるように
正しく関連付けられたネットワーク。
* 未使用のスイッチポートをすべて無効にします。
フォールトトレラント接続を必要とする
スイッチ間。
必要な変更のみ行ってください
上記の要件を完了してください。

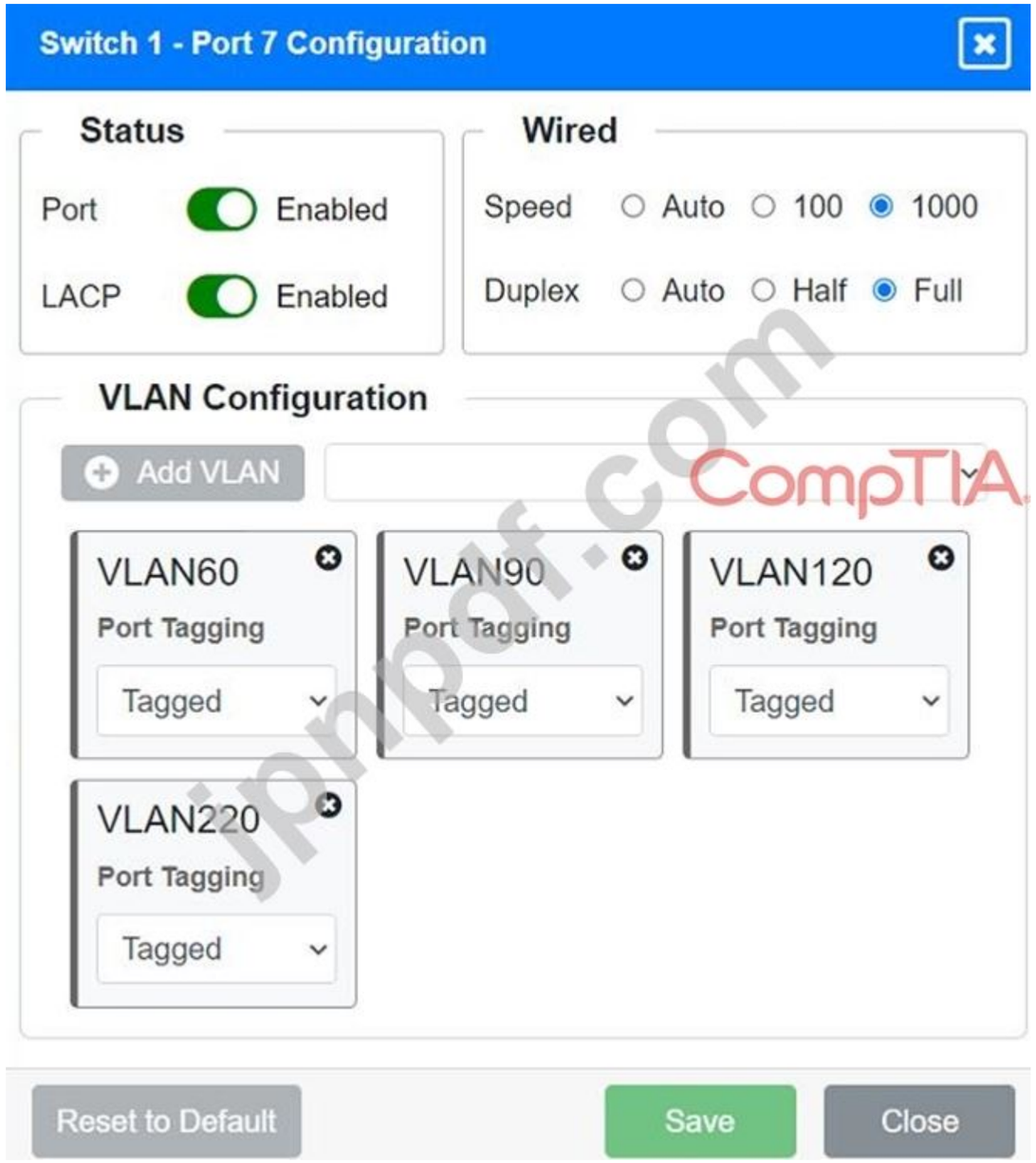


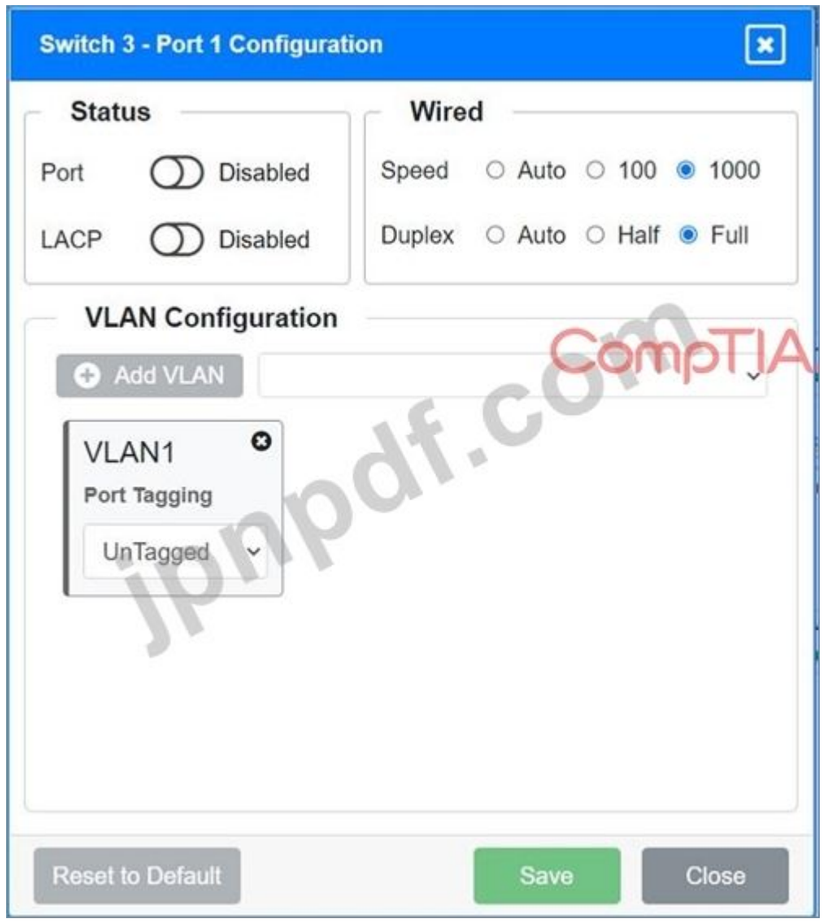
CompTIA


Switch 1 - Port 2 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 4 Configuration
CompTIA
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN90
Port Tagging
UnTagged
Reset to Default
Save
Close

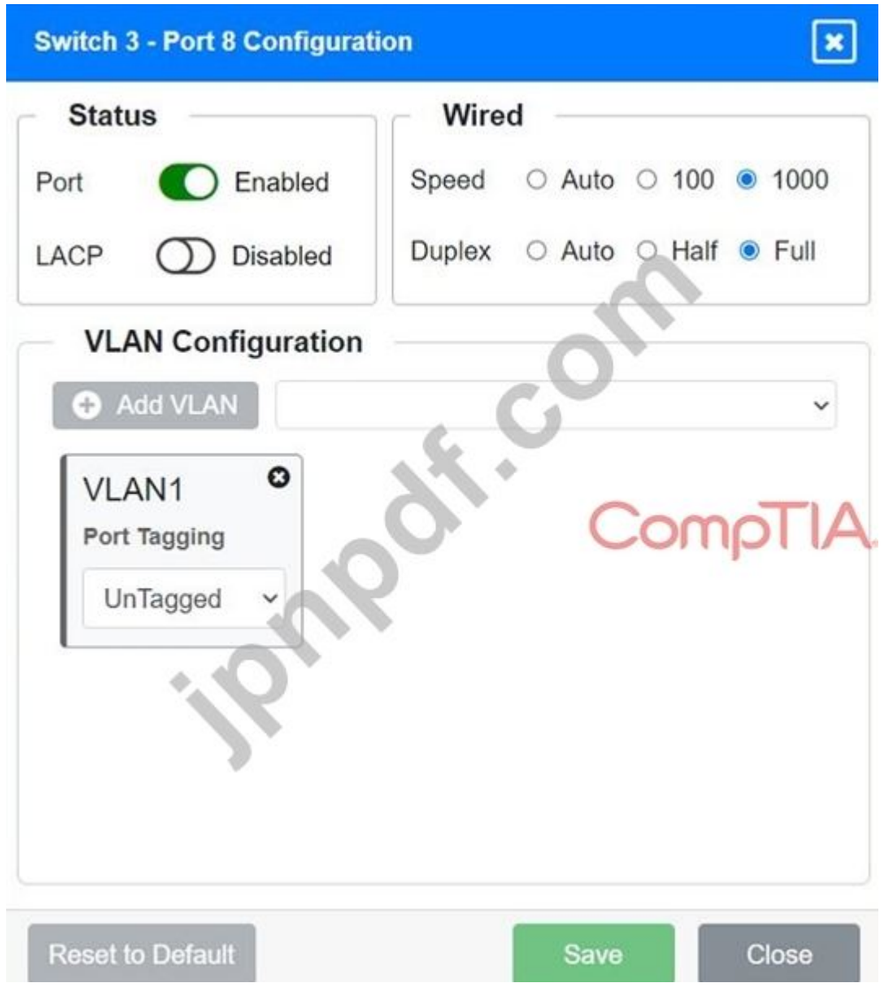

Switch 1 - Port 6 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 7 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close




Switch 3 - Port 2 Configuration
CompTIA
Status
Port
Disabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Reset to Default
Save
Close


Switch 3 - Port 5 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Reset to Default
Save
Close



Answer:

下記の説明の解決策を参照してください

Explanation:

アクセス レイヤー スイッチを構成するための完全なソリューションを提供するには、次の手順に従います。

各デバイスとポートの正しい VLAN を識別します。

必要なポートを有効にし、使用しないポートを無効にします。

スイッチ間のフォールトトレラント接続を構成します。

構成の詳細

スイッチ1

ポート 1 の構成 (コア スイッチへのアップリンク)

ステータス: 有効

LACP: 有効

速度: 1000

デュプレックス: フル

VLAN 設定: VLAN60、VLAN90、VLAN120、VLAN150、VLAN220 のタグ付き ポート 2 設定 (コア スイッチへのアップリンク) ステータス: 有効 LACP: 有効 速度: 1000 デュプレックス: フル VLAN 設定: VLAN60、VLAN90、VLAN120、VLAN150、VLAN220 のタグ付き ポート 3 設定 (サーバ接続) ステータス: 有効 LACP: 無効 速度: 1000 デュプレックス: フル VLAN 設定: VLAN90 (サーバ) のタグなし ポート 4 設定 (サーバ接続) ステータス: 有効 LACP: 無効 速度: 1000 デュプレックス: フル VLAN 設定: VLAN90 (サーバ) のタグなし ポート 5 設定 (有線ユーザおよび WLAN) ステータス: 有効 LACP: 有効 速度: 1000 デュプレックス: フル VLAN 設定: VLAN60、VLAN120、VLAN150 のタグ付き ポート 6 設定 (有線ユーザおよび WLAN) ステータス: 有効 LACP:有効 速度: 1000 デュプレックス: フル VLAN

設定: VLAN60、VLAN120、VLAN150 のタグ付き ポート 7 設定 (音声および有線ユーザー) ステータス: 有効 LACP: 有効 速度: 1000 デュプレックス: フル VLAN 設定:
VLAN60、VLAN90、VLAN120、VLAN220 のタグ付き ポート 8 設定 (音声、プリンター、および有線ユーザー) ステータス: 有効 LACP: 有効 速度: 1000 デュプレックス: フル VLAN 設定:
VLAN60、VLAN90、VLAN120、VLAN220 のタグ付き スイッチ 3 ポート 1 設定 (未使用) ステータス: 無効 LACP: 無効 ポート 2 設定 (未使用) ステータス: 無効 LACP: 無効 ポート 3 設定 (デバイスへの接続) ステータス: 有効 LACP: 無効 速度: 1000 デュプレックス: フル VLAN 設定: VLAN1 のタグなし (デフォルト) ポート 4 設定 (デバイスへの接続) ステータス: 有効LACP: 無効、速度: 1000、デュプレックス: フル、VLAN 設定: VLAN1 のタグなし (デフォルト)、ポート 5 の設定 (デバイスへの接続) ステータス: 有効、LACP: 無効、速度: 1000、デュプレックス: フル、VLAN 設定: VLAN1 のタグなし (デフォルト)、ポート 6 の設定 (デバイスへの接続) ステータス: 有効、LACP: 無効、速度: 1000、デュプレックス: フル、VLAN 設定: VLAN1 のタグなし (デフォルト)、ポート 7 の設定 (デバイスへの接続) ステータス: 有効、LACP: 無効、速度: 1000、デュプレックス: フル、VLAN 設定: VLAN1 のタグなし (デフォルト)、設定の概要、スイッチ 1 のポート 1 および 2 は、必要なすべての VLAN に対して VLAN タグ付けが有効になっているトランク ポートとして設定されています。
スイッチ 1 のポート 3 と 4 は、タグなし VLAN 90 を使用したサーバー接続用に構成されています。
スイッチ 1 のポート 5、6、7、および 8 は、複数の VLAN へのアクセスを必要とするデバイス用に構成されています。
スイッチ 3 の未使用ポートは無効になります。
スイッチ 3 のポート 3、4、5、6、および 7 は、デフォルトの VLAN 1 に対して有効になっています。
すべてのスイッチとポートが要件に従って構成されていることを確認します。
コア スイッチ ポートは、スイッチ 1 へのアップリンクに応じて必要に応じて設定する必要があります。
スイッチ間のトランク ポートの冗長性を確保するために、LACP が有効になっていることを確認します。
これらの構成に従うことで、各デバイスは正しく関連付けられたネットワークのみにアクセスし、未使用のスイッチ ポートは無効になり、スイッチ間にフォールト トレラント接続が確立されます。

最新問題**: 71**
ある会社では、サーバーへのすべての接続を暗号化する必要があるセキュリティをホストしています。ジュニア管理者は、Web サーバーをハード化する必要があります。Web サーバー上の次のポート。Web サーバー上の次のポートが開いています。

443
80
22
587

次のポートのうちどれを無効にする必要がありますか?
A. 22
B. 80
C. 443
D. 587
Answer: (解答を表示する**)**
すべての接続を暗号化する必要がある Web サーバーの場合は、ポート 80 (HTTP) を無効にする必要があります。ポート 80 は暗号化されていない Web トラフィックに使用され、ポート 443 は暗号化された通信を提供する HTTPS に使用されます。
* ポート 80 (HTTP): このポートは、セキュリティ保護されていない Web トラフィックに使用されます。このポートを無効にすると、すべての Web トラフィックで HTTPS が使用され、転送中のデータが暗号化されます。
* ポート 443 (HTTPS): このポートは、SSL/TLS 暗号化による安全な Web トラフィックに使用されます。このポートを開いたままにしておくと、Web サーバーへの安全な接続が確立されます。
* その他のポート:
* ポート 22: SSH に使用され、安全なリモート アクセスとファイル転送を提供します。
* ポート 587: 暗号化された安全な電子メール送信 (SMTP) に使用されます。
ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: さまざまなポートとプロトコルの役割とセキュリティ上の影響を説明します。
* Cisco Networking Academy: 安全な Web サーバーの構成とポート管理に関するトレーニングを提供します。

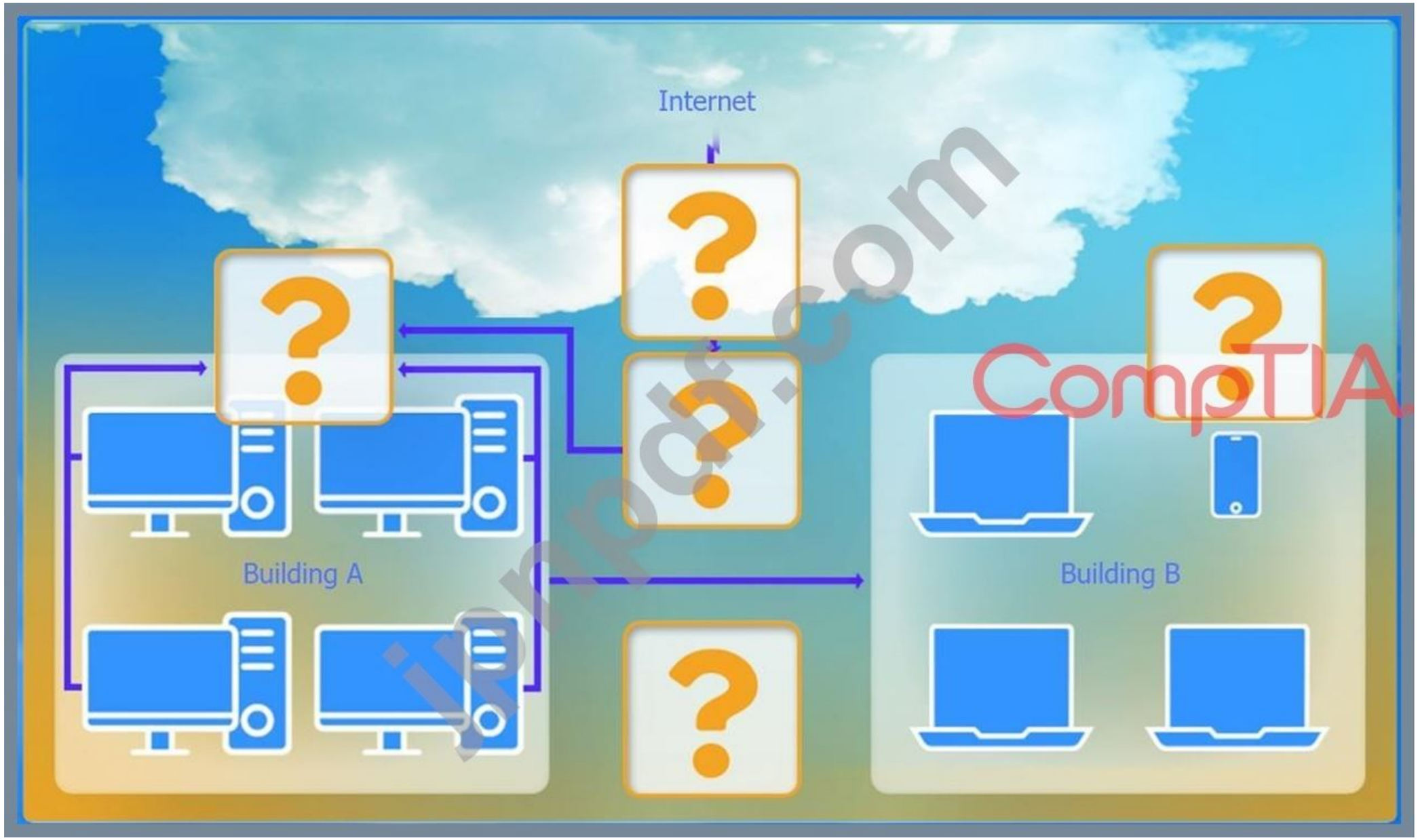
* Network+ 認定オールインワン試験ガイド: ポート セキュリティと Web サーバーを保護するためのベスト プラクティスについて説明します。

最新問題: **72**
トラブルシューティング方法論の次の手順のうち、最近の変更についてログを確認する手順はどれですか?
A. 原因を特定するために理論をテストします。
B. 問題を特定します。
C. 調査結果と結果を文書化します。
D. 行動計画を立てます。
Answer: B (メーッセージを残す**)**

最新問題: **73**
問題が特定された後、トラブルシューティング方法論の次のステップのうち、OSI モデルの各レベルをチェックする可能性が高いのはどれですか。
A. 理論を確立する。
B. ソリューションを実装します。
C. 行動計画を作成します。
D. 機能を検証します。
Answer: D (メーッセージを残す**)**
* トラブルシューティング方法の紹介:
* ネットワークのトラブルシューティングには、ネットワークの問題を特定して解決するための体系的なアプローチが含まれます。CompTIA Network+ 認定では、構造化されたトラブルシューティング方法論を重視しています。
* トラブルシューティングの手順:
* 問題を特定する: 情報を収集し、症状を特定し、ユーザーに質問します。
* 考えられる原因の理論を確立する: 問題の考えられる原因を検討します。
* 原因を特定するために理論をテストする: テストで理論を検証します。
* 問題を解決し、解決策を実行するための行動計画を立てる:
* 解決計画を実行する。
* 機能性を検証し、予防策を実施します。ソリューションが機能することを確認し、再発を防止します。
* 機能の検証:
* ソリューションを実装した後、機能を検証することで問題が完全に解決されたことが保証されます。
これには、ネットワークが正しく動作することを確認するためのテストが含まれます。
* OSI モデルの各レベルをチェックすることで、さまざまなレイヤー (物理、データ リンク、ネットワーク、トランスポート、セッション、プレゼンテーション、アプリケーション) における潜在的な問題がすべて解決されることを確認できます。
* オプションの説明:
* A. 理論を確立する: このステップでは、機能性を検証するのではなく、考えられる原因を仮説します。
* B. ソリューションを実装する: このステップでは、解決計画を実行します。
* C. 行動計画を作成する: このステップでは、検証ではなく解決策の計画を行います。
* D. 機能の検証: このステップでは、問題が完全に解決されていることを確認するために、OSI モデル レイヤーを含む包括的なチェックが行われます。
* 結論 :
* 機能の検証はトラブルシューティング プロセスにおける重要なステップであり、ソリューションの実装後にネットワークが正しく動作することを確認します。これには、すべての OSI モデル レイヤーにわたる徹底的なテストが含まれます。

参考文献:
* トラブルシューティングの方法論と機能の検証の重要性について説明した CompTIA Network+ ガイド (Ref 9f 基本設定コマンドのページを参照)。

最新問題**: 74**
ネットワーク管理者は、新しい企業オフィスのネットワークを構成する任務を負っています。オフィスは 2 つの建物で構成されており、物理的に接続されておらず、50 フィート離れています。構成は次の要件を満たす必要があります。
両方の建物のデバイスは
インターネットにアクセスできます。
セキュリティは、すべてのインターネットトラフィック
入場前に検査を受ける
ネットワーク。
デスクトップではトラフィックは表示されません
他のデバイス向け。
説明書
各場所に適切なネットワーク デバイスを選択します。該当する場合は、構成の更新が必要なデバイスの横にある虫眼鏡をクリックし、必要な変更を加えます。
すべてのデバイスが使用されるわけではありませんが、すべての場所を入力する必要があります。
いつでもシミュレーションの初期状態に戻したい場合は、 すべてリセット」ボタンをクリックしてください。


Internet
Building A
Building B

Hub

Switch

WAP

Firewall

Router

Wireless range extender

Wireless range extender settings

Basic Configuration

Access Point Name	WAP extender
Gateway	192.168.0.1
SSID	CORP
SSID Broadcast	Yes No

Wireless

Mode	
Channel	

Wired

Speed	Auto 100 1000
Duplex	Auto Half Full

Security Configuration

Security Settings	None WEP WPA WPA2 WPA2 - Enterprise
Key or Passphrase	N@En71$90*Ha

Reset to Default | Save | Close

Answer:

以下のステップバイステップの完全な解決策を参照してください。

Explanation:

* 両方の建物内のデバイスはインターネットにアクセスできる必要があります。
* セキュリティでは、すべてのインターネット トラフィックがネットワークに入る前に検査されることが求められます。
* デスクトップでは、他のデバイス宛のトラフィックは表示されません。

修正されたレイアウトと説明は次のとおりです。

* A棟:
* スイッチ: すべてのデスクトップを接続するために正しく配置されています。
* ファイアウォール: すべての受信トラフィックと送信トラフィックを検査できるように正しく配置されています。
* B棟:
* スイッチ: 必要ありません。代わりに、ワイヤレス アクセス ポイント (WAP) を配置して、ラップトップやモバイル デバイスにワイヤレス接続を提供します。
* 建物間:
* ワイヤレス範囲拡張器: 建物間のワイヤレス接続を提供するために適切に配置されています。
* インターネットへの接続:
* ルーター: インターネットに接続し、建物とインターネット間のトラフィックをルーティングするために適切に配置します。
* ファイアウォール: ファイアウォールは、ルータと内部ネットワークの間に配置して、ネットワークに入る前にすべてのトラフィックを検査する必要があります。

修正されたセットアップ:

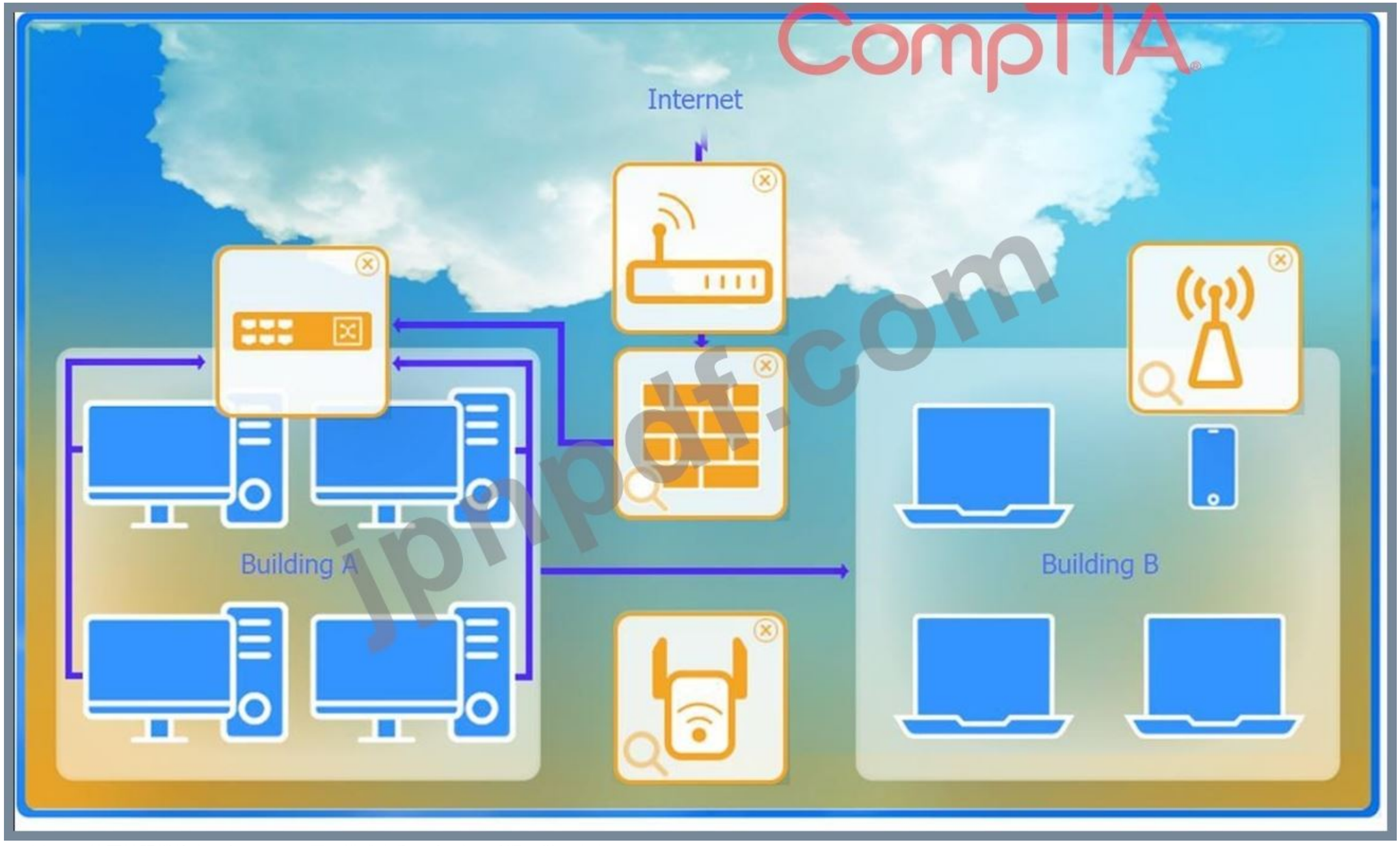
* 左上（建物A）スイッチ
* 左下（建物A）ファイアウォール（ネットワークに入る前にトラフィックを検査する）
* 上中段（インターネット接続）ルーター
* 下中段（建物の間）ワイヤレスレンジエクステンダー
* 右上（建物B）ワイヤレスアクセスポイント（WAP）

この修正された設定では、建物 B の WAP は、ルーターに接続されたワイヤレス レンジ エクステンダーにワイヤレスで接続します。ルーターはファイアウォールに接続されており、すべてのトラフィックがネットワークに入る前に検査されるようになっています。

ワイヤレスレンジエクステンダーの構成:

* SSID: 株式会社
* セキュリティ設定: WPA2 または WPA2 - エンタープライズ
* キーまたはパスフレーズ: [強力なパスフレーズを入力してください]
* モード: [ネットワークプランに基づいて設定]
* チャンネル: [ネットワークプランに応じて設定]
* 速度: 自動
* 両面印刷: 自動

これらの設定により、両方の建物からインターネットに安全にアクセスでき、すべてのトラフィックはネットワークに入る前にファイアウォールによって検査されます。デスクトップやその他のデバイスには、他のユーザー宛のトラフィックが表示されず、必要なセキュリティとプライバシーが維持されます。



ワイヤレス範囲拡張機能をセキュリティ用に構成するには、次の手順に従います。
* SSID (サービス セット識別子):
* 図に示すように、SSID が 「CORP」に設定されていることを確認します。
* セキュリティ設定:
* WPA2 または WPA2 - エンタープライズ: セキュリティを強化するには、これらのオプションのいずれかを選択します。
WPA2-Enterprise は、集中認証によるより強力なセキュリティを提供するため、企業環境に最適です。
* キーまたはパスフレーズ:
* WPA2 を選択した場合は、 「キーまたはパスフレーズ」フィールドに強力なパスフレーズを入力します。

* WPA2 - Enterprise を選択した場合は、図には示されていない RADIUS などの認証サーバーの追加設定を構成する必要があります。
* ワイヤレスモードとチャネル:
* 干渉を避けるため、ネットワーク設計や環境に応じて適切なモードとチャネルを設定してください。これらの設定は展示では指定されていないため、ネットワーク計画に従って設定してください。
* 有線速度とデュプレックス:
* 100 Mbps または 1000 Mbps の特定の要件がない限り、速度を 「自動」に設定します。
* ネットワーク機器に基づいて半二重または全二重を指定する必要がない限り、デュプレックスを 「自動」に設定します。
* 設定を保存:
* 必要な変更を行った後、 「保存」ボタンをクリックして設定を適用します。
調整後の構成は次のようになります。
* SSID: 株式会社
* セキュリティ設定: WPA2 または WPA2 - エンタープライズ
* キーまたはパスフレーズ: [強力なパスフレーズを入力してください]
* モード: [ネットワークプランに基づいて設定]
* チャンネル: [ネットワークプランに応じて設定]
* 速度: 自動
* 両面印刷: 自動
これらの設定が構成されると、ワイヤレス範囲拡張機能によって両方の建物内のデバイスに安全な接続が提供されます。
ファイアウォール設定で要件とセキュリティのベストプラクティスに完全に準拠するには、次の調整と追加を検討してください。
* DNS ルール: このルールは、内部ネットワークから任意の宛先への DNS トラフィックを許可します。これは問題ありません。
* HTTPS送信: このルールは、内部ネットワークからのHTTPSトラフィックを許可します（
192.169.0.1/24 はタイプミスで、192.168.0.1/24 とする必要があります) を任意の宛先に提供できるため、安全な Web ブラウジングにも適しています。
* 管理: このルールは、管理タスクに必要な管理目的でファイアウォールへの SSH アクセスを許可します。
* HTTPS 受信: このルールは、内部ネットワークへの受信 HTTPS トラフィックを拒否します。これは、インターネットからアクセスする必要がある Web サーバーがない限り適切です。
* HTTP 受信: このルールは、内部ネットワークへの受信 HTTP トラフィックを拒否します。これはセキュリティ上の目的に適しています。
推奨される追加設定:
* 一般的な送信トラフィックを許可: Web アクセス、電子メールなどの一般的な送信トラフィックを許可します。
* その他のすべてのトラフィックをブロック: 不正アクセスを防ぐために、その他のすべてのトラフィックがブロックされていることを確認します。
ファイアウォール構成の調整:
* ネットワークのタイプミスを修正します:
* サブネット 192.169.0.1/24 が 192.168.0.1/24 に修正されていることを確認します。
* 一般的な送信トラフィックを許可する:
* ルール名: 一般送信
* ソース: 192.168.0.1/24
* 目的地: 任意
* サービス: 任意
* アクション: 許可
* その他のすべてのトラフィックを拒否:
* ルール名: すべてブロック
* 出典: ANY
* 目的地: 任意

* サービス: 任意
* アクション: 拒否
更新されたファイアウォール設定は次のようになります。
ルール名
ソース
行き先
サービス
アクション
DNSルール
192.168.0.1/24
どれでも
ドメイン名
許可する
HTTPS 送信
192.168.0.1/24
どれでも
翻訳
許可する
管理
どれでも
192.168.0.1/24
パスワード
許可する
HTTPS 受信
どれでも
192.168.0.1/24
翻訳
拒否
HTTP 受信
どれでも
192.168.0.1/24
ウェブ
拒否
一般アウトバウンド
192.168.0.1/24
どれでも
どれでも
許可する
すべてブロック
どれでも
どれでも
どれでも

どれでも
拒否
これらの設定により、次のことが保証されます。
* 内部デバイスは外部から DNS および HTTPS サービスにアクセスできます。
* SSH経由の管理アクセスが許可されます。
* 特に指定がない限り、受信 HTTP および HTTPS トラフィックは拒否されます。
* 一般的な送信トラフィックは許可されます。
* その他のトラフィックはすべてデフォルトでブロックされ、安全な環境が確保されます。
調整を行った後は必ず設定を保存してください。

最新問題: **75**
次のファイバー コネクタ タイプのうち、ネットワーク インターフェイス カードで使用される可能性が最も高いのはどれですか。
A. LC
B. SC
C. ST
D. MPO
Answer: (解答を表示する**)**
* ファイバーコネクタタイプの定義:
* LC (Lucent コネクタ): プッシュプル ラッチ機構を備えた小型フォームファクタの光ファイバー コネクタ。高密度アプリケーションでよく使用されます。
* SC (加入者コネクタまたは標準コネクタ): プッシュプルラッチ機構を備えた大型フォームファクタコネクタ。データ通信や電気通信アプリケーションでよく使用されます。
* ST (ストレート チップ): バヨネット スタイルのコネクタ。通常はマルチモード光ファイバー ネットワークで使用されます。
* MPO（マルチファイバープッシュオン）：複数ファイバー（通常2または24）をサポートするように設計されたコネクタ。
* 高密度ケーブル環境で使用される光ファイバーです。
* 一般的な使用法:
* LC コネクタ: LC コネクタはサイズが小さいため、ネットワーク インターフェイス カード (NIC) やデータ センターなどの高密度環境で広く使用されています。SC コネクタや ST コネクタに比べて、より狭いスペースでより多くの接続が可能になります。
* SC および ST コネクタ: これらはより大きく、パッチ パネルや古いファイバー インストールでよく使用されますが、高密度アプリケーションには適していません。
* MPO コネクタ: 主にデータ センターや高密度アプリケーションのトランク ケーブルに使用されますが、個々のネットワーク インターフェイス カードでは通常使用されません。
* 選考基準:
* LC コネクタは、小型フォームファクタと高密度機能を備えているため、スペースと接続密度が重要な考慮事項となるネットワーク インターフェイス カードに最適です。
参考文献:
* 光ファイバーとコネクタの種類に関する CompTIA Network+ 学習教材。

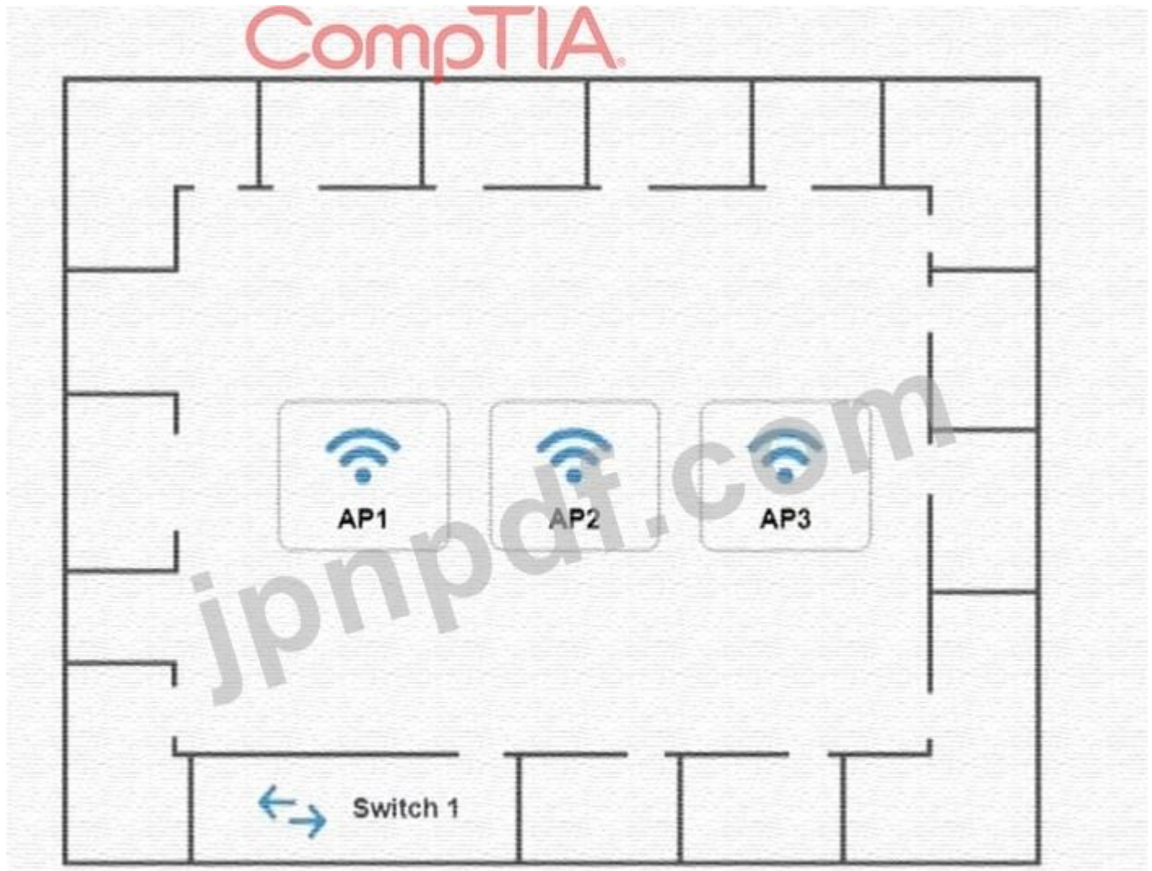
最新問題: **76**
ネットワーク管理者は、35 台の PoE セキュリティ カメラを設置中です。管理者は、新しいケーブルを設置してテストした後、カメラを設置しました。しかし、少数のカメラが動作しません。最も大きな原因は次のどれですか。
A. 配線規格が正しくありません
B. 電力予算を超過しました
C. 信号減衰
D. 電圧が間違っています

Answer: B (メーッセージを残す)
セキュリティ カメラなどの複数の Power over Ethernet (PoE) デバイスを設置する場合、総電力要件が PoE スイッチの電力バジェットを超えないようにすることが重要です。各 PoE スイッチには最大電力容量があり、この容量を超えると一部のデバイスが電力を受信できなくなる可能性があります。
* PoE 規格: PoE スイッチは、IEEE 802.3af (PoE) や 802.3at (PoE+) などの規格に準拠しており、それぞれポートごとの特定の電力制限と総電力容量が定められています。
* 電力計算: 接続されているすべての PoE デバイスの電力要件を合計すると、スイッチの合計電力予算を超えているかどうかを判断するのに役立ちます。
* 症状: 電力バジェットを超過すると、一部のデバイス (通常はスイッチから最も遠いデバイスや最後に接続されたデバイス) の電源が入らないか、正しく機能しない場合があります。
ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: PoE 標準と電源の問題のトラブルシューティングについて説明します。
* Cisco Networking Academy: PoE テクノロジー、電力予算、PoE デバイスの管理について説明します。
* Network+ 認定オールインワン試験ガイド: 電力予算の考慮事項を含む PoE セットアップに関する情報を提供します。

最新問題**: 77**
ネットワーク管理者は新しいスイッチを導入しており、スパニング ツリーのデフォルトの優先度値が設定されていることを確認したいと考えています。ネットワーク管理者は次のどの値が表示されると予想しますか。
A. 4096
B. 8192
C. 32768
D. 36684
Answer: C (メーッセージを残す)
スパニングツリープロトコル (STP) について理解する:
STP は、一部の冗長パスを選択的にブロックするスパニング ツリーを作成することにより、イーサネット ネットワークでのネットワーク ループを防ぐために使用されます。
デフォルトの優先度値:
ブリッジ プライオリティ: STP はブリッジ プライオリティを使用して、どのスイッチがルート ブリッジになるかを決定します。ほとんどのスイッチのデフォルトのブリッジ プライオリティ値は 32768 です。
優先度の範囲: ブリッジ優先度は 0 ～ 61440 の範囲で 4096 単位で設定できます。
構成と検証:
新しいスイッチを導入する場合、ネットワーク管理者は show spanning-tree などのコマンドを使用してブリッジの優先順位を確認し、それがデフォルト値の 32768 に設定されているかどうかを確認できます。
他の値との比較:
4096 および 8192: デフォルトの優先度よりも低いため、手動で優先度を高く設定する必要があることを示します。
36684: 非標準の値。特定の構成変更の結果である可能性があります。
参照 :
スパニング ツリー プロトコルとネットワーク構成に関する CompTIA Network+ 学習教材。

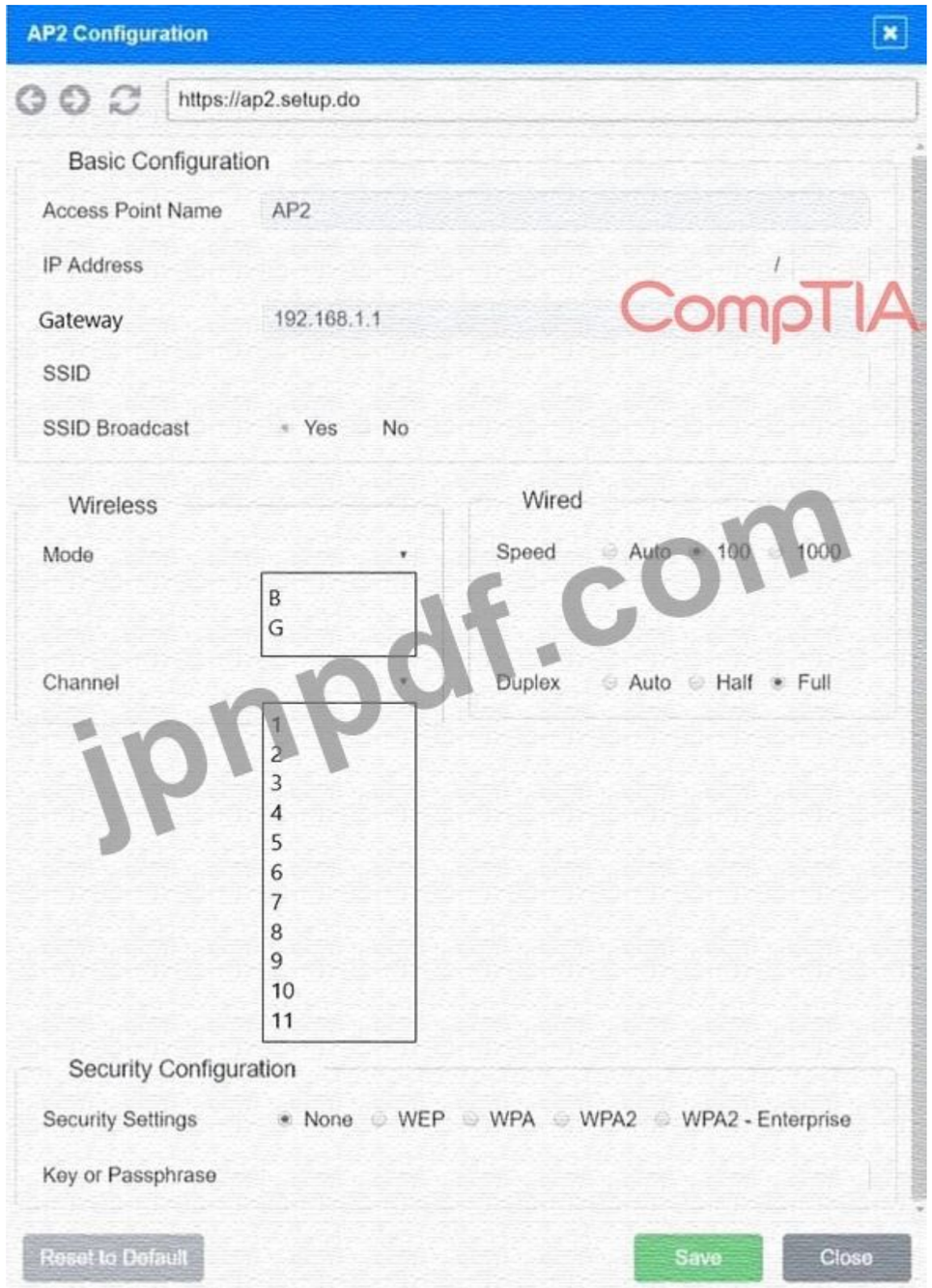
最新問題: **78**
コストを削減し、モビリティを向上させるために、最高技術責任者 (CTO) は、組織とその関連会社にクラウド サービスを導入したいと考えています。ユーザーへの影響を軽減するために、CTO は主要なサービスをオンサイト データ センターから実行し、エンタープライズ サービスをクラウドで実行したいと考えています。次の展開モデルのどれが組織にとって最適な選択でしょうか。
A. パブリック
B. ハイブリッド
C. SaaS
D. プライベート
Answer: B (メーッセージを残す**)**
ハイブリッド クラウド導入モデルは、CTO の要件に最適な選択肢です。このモデルでは、組織はオンサイト データ センターから主要なサービスを実行しながら、エンタープライズ サービスにクラウドを活用できます。このアプローチは、柔軟性、拡張性、コスト削減を実現すると同時に、重要なサービスをローカルに維持することでユーザーへの影響を最小限に抑えます。ハイブリッド モデルは、プライベート クラウド環境とパブリック クラウド環境の両方を統合し、両方の利点を提供します。参考資料: CompTIA Network+ 学習教材およびクラウド コンピューティングの原則。

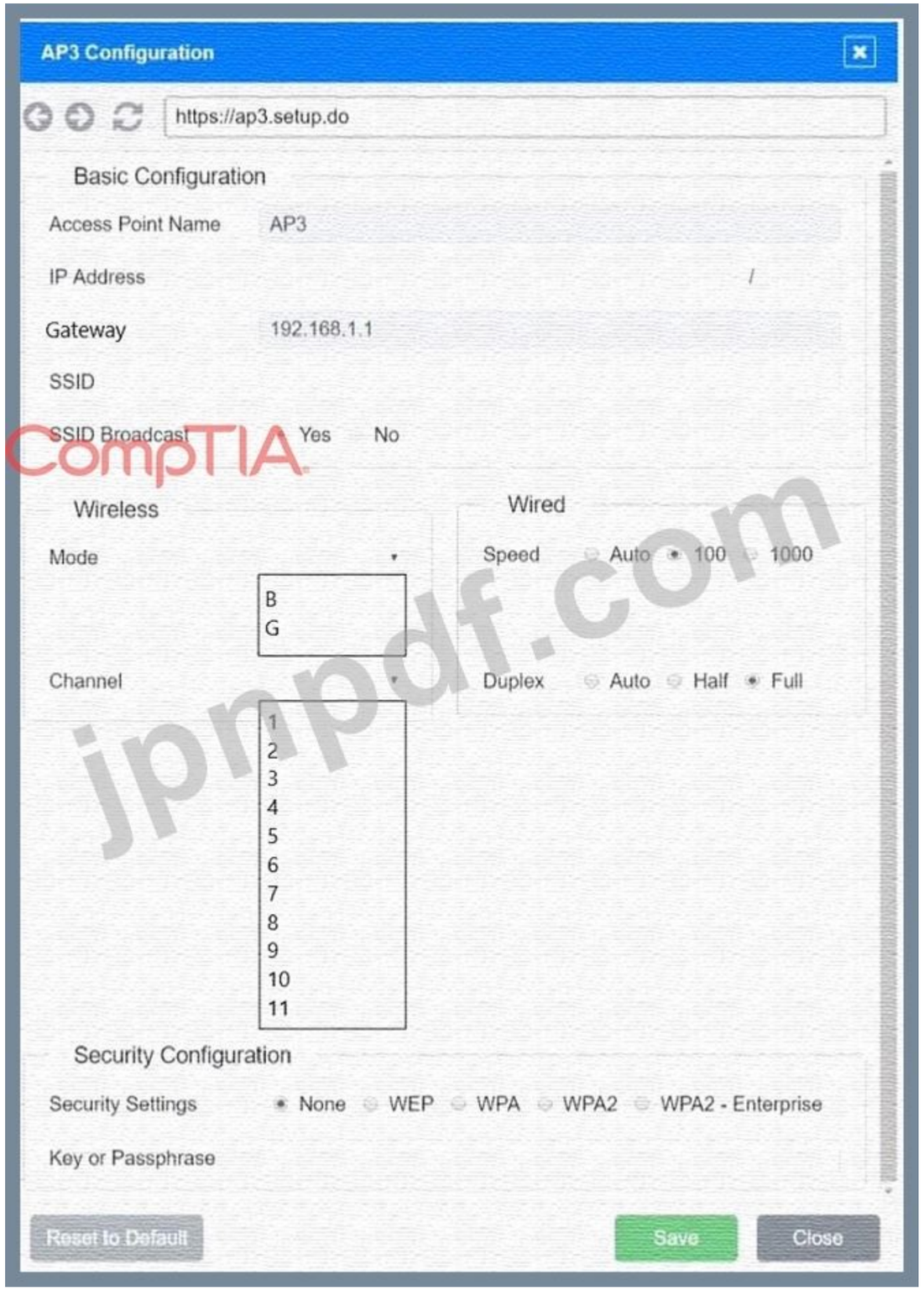
最新問題: **79**
シミュレーション
オフィスにワイヤレス ネットワークを設定するという任務を負っています。ネットワークは 3 つのアクセス ポイントと 1 つのスイッチで構成されます。ネットワークは次のパラメータを満たす必要があります。
SSID は、S3cr3t のキーを使用して CorpNet として設定する必要があります。
無線信号は互いに干渉し合ってはならない
アクセス ポイントとスイッチが接続されているサブネットは、最大 30 台のデバイスのみをサポートする必要があります。アクセス ポイントは、TKIP クライアントを最大速度でのみサポートするように構成する必要があります。手順: ワイヤレス デバイスをクリックしてその情報を確認し、アクセス ポイントの設定を特定の要件に合わせて調整します。
いつでもシミュレーションの初期状態に戻したい場合は、すべてリセット」ボタンをクリックしてください。



192.168.1.2
Speed: Auto
Duplex: Auto


AP1 Configuration
https://ap1.setup.do
Basic Configuration
Access Point Name
AP1
IP Address
/
Gateway
192.168.1.1
SSID
SSID Broadcast
Yes
No
Wireless
Mode
B
G
Channel
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
Reset to Default
Save
Close





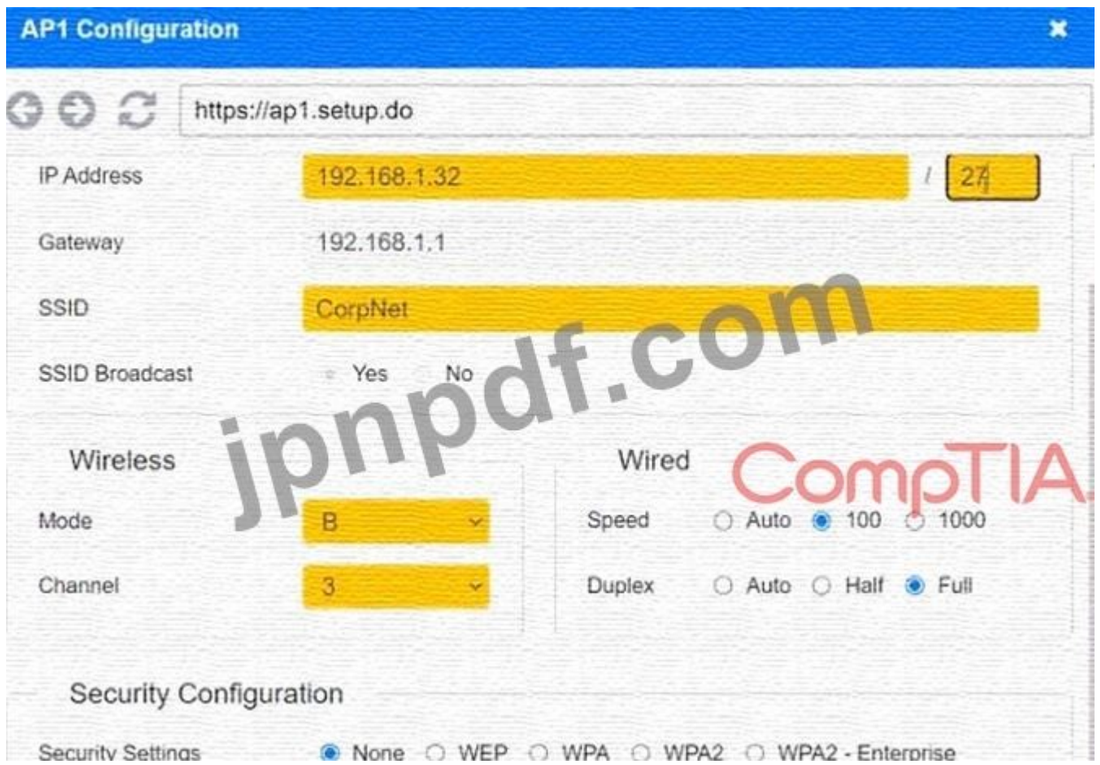
Answer:

下記の説明を参照してください。

Explanation:
最初の展示では、レイアウトは次のようになります

グラフィカルユーザーインターフェイス、テキスト、アプリケーション、チャット、またはテキストメッセージの説明が自動的に生成されます

グラフィカルユーザーインターフェースの説明は自動的に生成されます



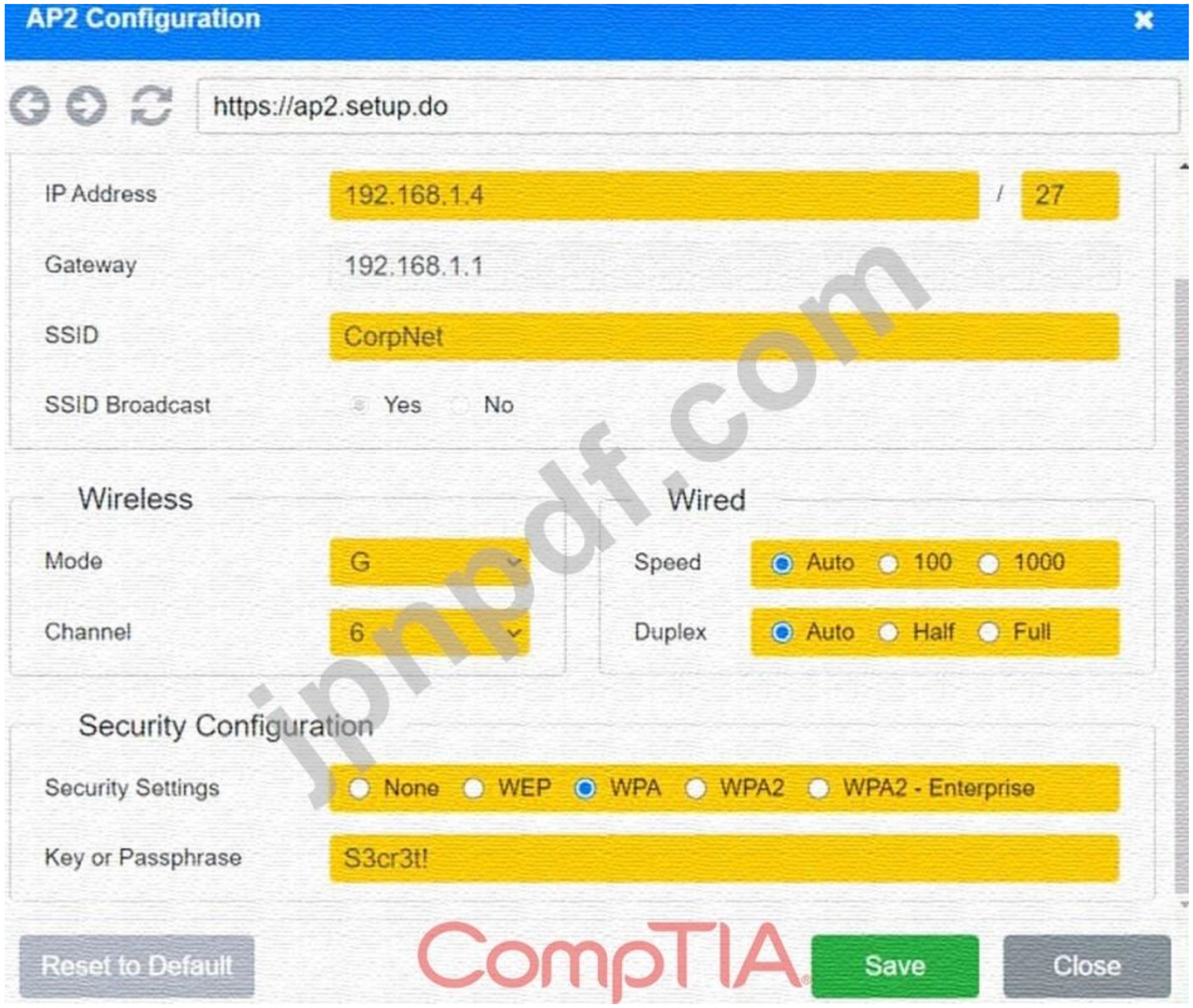
グラフィカルユーザーインターフェイス、テキスト、アプリケーション、チャット、またはテキストメッセージの説明が自動的に生成されます

グラフィカルユーザーインターフェースの説明は自動的に生成されます

別紙2は以下のとおり
アクセスポイント名 AP2
グラフィカルユーザーインターフェースの説明は自動的に生成されます

グラフィカルユーザーインターフェイス、テキスト、アプリケーション、チャット、またはテキストメッセージの説明が自動的に生成されます

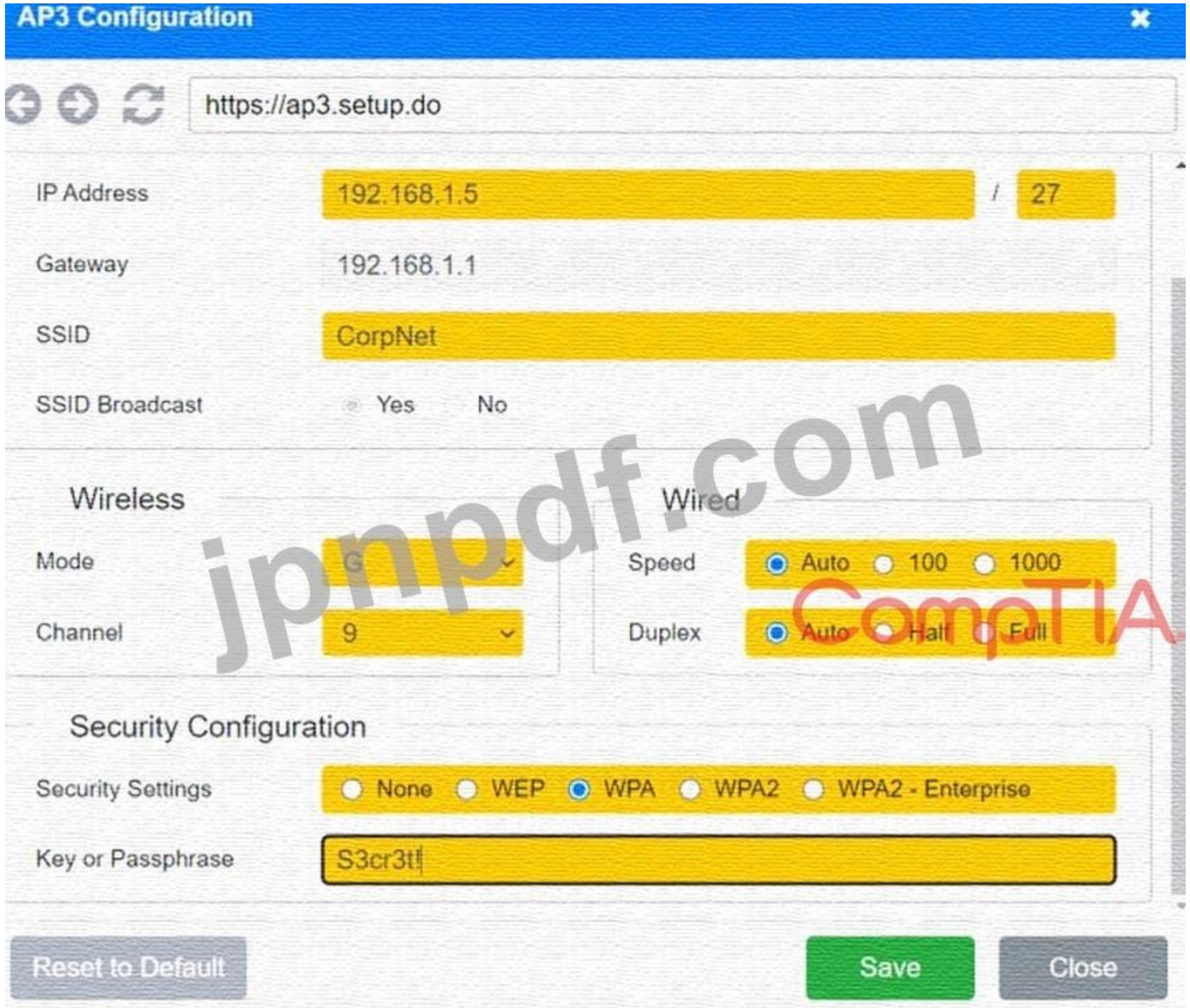
グラフィカルユーザーインターフェースの説明は自動的に生成されます



別添3は以下のとおり
アクセスポイント名 AP3
グラフィカルユーザーインターフェースの説明は自動的に生成されます

グラフィカルユーザーインターフェイス、テキスト、アプリケーション、チャット、またはテキストメッセージの説明が自動的に生成されます

グラフィカルユーザーインターフェースの説明は自動的に生成されます



最新問題: **80**
次のクラウド サービス モデルのうち、データ センターをクラウドに移行する際に顧客による初期費用が最も高くなる可能性が高いのはどれですか。
A. サービスとしてのネットワーク
B. サービスとしてのインフラストラクチャ
C. サービスとしてのソフトウェア
D. サービスとしてのプラットフォーム
Answer: B (メーッセージを残す**)**
最新問題: **81**

攻撃の一環として、脅威の攻撃者はスイッチ上のコンテンツ アドレス可能メモリ (CAM) テーブルを意図的にオーバーフローさせます。このシナリオは、次のどのタイプの攻撃の例ですか。
A. ARPスプーフィング
B. 邪悪な双子
C. MACフラッディング
D. DNS ポイズニング
Answer: C (メーッセージを残す**)**
* MACフラッディングの定義:
* MAC フラッディングは、悪意のある攻撃者が多数の偽の MAC アドレスをスイッチに送信し、スイッチの CAM テーブルを圧倒する攻撃です。CAM テーブルには、トラフィックの効率的な転送のために、MAC アドレスとそれに関連付けられたポートが保存されます。
* MACフラッディングの影響:
* CAM テーブル オーバーフロー: CAM テーブルがいっぱいになると、スイッチは新しい MAC アドレスを学習できず、すべてのポートにトラフィックをブロードキャストしなければならなくなり、ネットワーク パフォーマンスが低下し、データが傍受される可能性があります。
* スイッチの動作: スイッチはフェールオープン モードで動作し、ネットワークをハブとして扱うため、トラフィックの盗聴に悪用される可能性があります。
* 他の攻撃との比較:
* ARP スプーフィング: 偽の ARP (アドレス解決プロトコル) メッセージを送信して、攻撃者の MAC アドレスを別のデバイスの IP アドレスに関連付けます。
* 悪魔の双子: 正規のワイヤレス アクセス ポイントを模倣した不正なワイヤレス アクセス ポイントを作成してデータを傍受します。
* DNS ポイズニング: 偽の情報で DNS キャッシュを破壊し、トラフィックを悪意のあるサイトにリダイレクトします。
* 予防策:
* ポート セキュリティ: スイッチのポート セキュリティを構成して、ポートあたりの MAC アドレスの数を制限し、CAM テーブルのオーバーフローを防止します。
* ネットワーク セグメンテーション:VLAN を使用してネットワーク トラフィックをセグメント化し、このような攻撃の影響を制限します。
参考文献:
* ネットワーク セキュリティの脅威と軽減技術に関する CompTIA Network+ 学習教材。

最新問題**: 82**
ネットワーク管理者は、企業ネットワークにセキュリティ ゾーンを実装して、企業内の個人のみのアクセスを制御したいと考えています。次のセキュリティ ゾーンのうち、最適なソリューションはどれですか。
A. エクストラネット
B. 信頼できる
C. VPN
D. パブリック
Answer: (解答を表示する**)**
* セキュリティゾーンの紹介:
* セキュリティ ゾーンは、セキュリティ ポリシーを適用し、アクセスを制御するために設計された、ネットワーク内の論理セグメントです。ネットワークのさまざまな部分を分離して保護するのに役立ちます。
* セキュリティゾーンの種類:
* 信頼ゾーン: これは最も安全なゾーンであり、通常は信頼できるユーザーのみがアクセスできる社内ネットワークに使用されます。
* エクストラネット: このゾーンでは、外部のパートナー、ベンダー、または顧客への制御されたアクセスが許可されます。
* VPN (仮想プライベートネットワーク): VPN はインターネット上で安全な接続を確立するために使用されますが、それ自体はセキュリティゾーンではありません。
* パブリック ゾーン: このゾーンは最も安全性が低く、通常は誰でもアクセスできるパブリック サービスに使用されます。
* 信頼ゾーンの実装:

* 信頼ゾーンは、社内のユーザーとリソースを含むように構成されています。アクセス制御、
* ファイアウォールやその他のセキュリティ対策により、許可された担当者のみがこのゾーンにアクセスできるようになります。
* 財務部門、人事部門、その他の重要な機能などの内部ネットワーク セグメントは、通常、信頼ゾーンに配置されます。
* 構成例:
* ファイアウォール ルール: 内部 IP アドレスからのトラフィックのみを許可するルールを設定します。
* アクセス制御リスト (ACL): ルータとスイッチに ACL を実装し、IP アドレスやその他の基準に基づいてアクセスを制限します。
* セグメンテーション:VLAN とサブネットを使用して、信頼できるゾーンを他のゾーンからセグメント化して分離します。
* オプションの説明:
* A. エクストラネット: 社内のみのアクセスではなく、外部パートナーに適しています。
* B. 信頼できる: 社内のユーザーに制御されたアクセスを提供するため、これが正解です。
* C. VPN: セキュリティゾーンそのものではなく、安全なリモートアクセスを実現する方法。
* D. パブリック: 社内ユーザーではなく、パブリック アクセスに適しています。
* 結論 :
* 信頼ゾーンを実装することは、企業ネットワーク内のアクセスを制御するための最適なソリューションです。
信頼できる内部ユーザーのみが機密リソースにアクセスできるようにすることで、ネットワーク セキュリティが強化されます。
参考文献:
* セキュリティ ゾーンと企業ネットワークにおけるその実装について詳しく説明した CompTIA Network+ ガイド (9 ページ 「基本設定コマンド」を参照)。

最新問題: 83
パススルー プラグを使用して Cat 8 ケーブルを配線した後、電気技師は接続されたケーブルでクロストークが頻繁に発生していることに気付きました。電気技師が最初に実行する必要があるトラブルシューティング手順は次のうちどれですか。
A. コネクタに接触または露出しているワイヤがないか検査します。
B. 接続されているデバイスのデフォルト設定を復元します。
C. 接続を再度終了します。
D. エリア内の無線周波数干渉を確認します。
Answer: A (メーッセージを残す)
クロストークは、ケーブルの不適切な終端処理によって発生することがよくあります。トラブルシューティングの最初の手順は、コネクタを検査して、接触または露出している可能性のあるワイヤがないかどうかを確認することです。すべてのワイヤが正しく接続され、導体が露出していないことを確認すると、クロストークを軽減または排除できます。この手順は、接続の再終端処理を試みたり、他の干渉源を確認したりする前に実行する必要があります。
参考: CompTIA Network+ 学習教材。

最新問題: 84
ユーザーは、IP アドレス 10.249.3.76 の内部 Web サイトに接続できません。ネットワーク管理者がコマンドを実行すると、次の出力が表示されます。
1 3ミリ秒 2ミリ秒 3ミリ秒 192.168.25.234
2 2ミリ秒 3ミリ秒 1ミリ秒 192.168.3.100
3 4ミリ秒 5ミリ秒 2ミリ秒 10.249.3.1
4 *
5'
6 *
7 *

ネットワーク管理者は、次のコマンドライン ツールのどれを使用していますか?
A. トレース
B. ネットスタット
C. tcpdump
D. nmap
Answer: (解答を表示する**)**
Tracert を理解する:
tracert (Windows では Traceroute) は、パケットが送信元から送信先までたどるパスを追跡するために使用されるコマンドライン ツールです。ルート (各ホップの特定のゲートウェイ) を記録し、IP ネットワーク上のパケットの転送遅延を測定します。
出力分析:
出力には、一連の IP アドレスと、それに対応するラウンドトリップ時間 (RTT) がミリ秒単位で表示されます。
アスタリスク (*) は、それらのホップから応答が受信されなかったことを示します。これは、tracert によって使用される ICMP パケットをブロックするルーターまたはファイアウォールの場合によく見られます。
他のツールとの比較:
netstat: ネットワーク接続、ルーティング テーブル、インターフェイス統計などを表示しますが、パケット ルートはトレースしません。
tcpdump: 分析用にネットワーク パケットをキャプチャし、詳細なネットワーク トラフィックの検査に使用します。
nmap: パケット ルートの追跡ではなく、ネットワーク上のホストとサービスを検出するために使用されるネットワーク スキャン ツール。
使用法：
tracert は、宛先へのパスを識別し、ネットワーク内の障害点や輻輳点を特定するのに役立ちます。
参照：
ネットワークのトラブルシューティングと診断ツールに関する CompTIA Network+ 学習教材。

最新問題**: 85**
最後のバックアップ以降に失われたデータの量を表すために使用される災害復旧メトリックは次のどれですか?
A. 平均所要時間
B. RTO
C. RPO
D. MTBF
Answer: C (メーッセージを残す**)**
RPO の定義:
リカバリ ポイント目標 (RPO) は、時間で測定されたデータ損失の最大許容量を表す災害復旧メトリックです。これは、災害後に通常の操作を再開するためにデータを復旧する必要がある時点を示します。
たとえば、RPO が 24 時間に設定されている場合、ビジネスでは中断が発生した場合に最大 24 時間分のデータが失われることを許容できます。
RPO が重要な理由:
RPO はバックアップ頻度を決定する上で重要であり、企業がデータをバックアップする必要がある頻度を決定するのに役立ちます。RPO が低いほど、バックアップの頻度が高くなり、データ損失の可能性が低くなります。
他の指標との比較:
MTTR (平均修復時間): システムまたはコンポーネントを修復して通常の動作に戻すのに必要な平均時間を指します。
RTO (目標復旧時間): 障害または災害が発生した後、コンピューター、システム、ネットワーク、またはアプリケーションがダウンしても許容される最大時間。
MTBF (平均故障間隔): 動作中のシステム固有の故障間の予測経過時間。

災害復旧における RPO の使用方法:
組織は、業務運営に許容できる時間枠内でデータを回復できるようにするために RPO を確立します。これには、RPO 要件を満たすバックアップ プランの作成が含まれます。
参照 :
CompTIA Network+ の学習教材と認定ガイド。

最新問題**: 86**
IT マネージャーは、メッシュ ネットワークで 10 個のサイトを接続する必要があります。各サイトは、プロビジョニング時間を短縮して保護する必要があります。次のテクノロジのうち、この要件を最もよく満たすものはどれですか。
A. SD-WAN
B. VXLAN
C. VPN
D. NFV
Answer: (解答を表示する**)**
* SD-WANの定義:
* ソフトウェア定義広域ネットワーク (SD-WAN) は、ネットワーク ハードウェアをその制御メカニズムから切り離すことで、WAN の管理と運用を簡素化するテクノロジです。これにより、集中管理とセキュリティの強化が可能になります。
* SD-WANの利点:
* プロビジョニング時間の短縮:SD-WAN により、集中管理と自動化により新しいサイトを迅速かつ簡単に展開できます。
* セキュリティ:暗号化、安全なトンネリング、統合ファイアウォールなどの高度なセキュリティ機能を組み込んでいます。
* スケーラビリティ: 追加のサイトや帯域幅の要件に合わせて簡単に拡張できます。
* 他の技術との比較:
* VXLAN (Virtual Extensible LAN):主にデータセンター内のネットワーク仮想化に使用されます。
* VPN (仮想プライベート ネットワーク): 安全な接続を提供しますが、SD-WAN のような集中管理とプロビジョニングの効率は提供されません。
* NFV (ネットワーク機能仮想化): ネットワーク サービスを仮想化しますが、WAN の管理とプロビジョニングには特に対応していません。
* 実装 :
* SD-WAN ソリューションは、各サイトにエッジ デバイスを展開し、中央コントローラに接続することで実装されます。これにより、動的ルーティング、トラフィック管理、セキュリティ ポリシーの適用が可能になります。
参考文献:
* CompTIA Network+ コース教材とネットワーク ソリューション ガイド。

最新問題**: 87**
ユーザーは Web ブラウザ経由で企業の VPN に接続し、TLS を使用して社内財務システムにアクセスし、タイムカードを入力できます。VPN の使用方法を最もよく表しているのは次のどれですか。
A. クライアントレス
B. クライアントからサイトへ
C. フルトンネル
D. サイト間
Answer: A (メーッセージを残す**)**
このシナリオでは、ユーザーが TLS を使用して Web ブラウザ経由で企業 VPN に接続し、内部システムにアクセスする方法について説明します。この設定は、「クライアントレス」VPN として最もよく説明されます。クライアントレス VPN では、ユーザーのデバイスに VPN クライアントをインストールする必要はなく、代わりに標準の Web ブラウザを使用して接続を確立します。この方法は、追加のソフトウェアをインストールすることなく、Web インターフェイスを介してアプリケーションへの安全なリモート アクセスを提供する場合に特に便利です。

参考: CompTIA Network+ 認定試験の目標 - リモート アクセス方法のセクション。

最新問題**: 88**
ある企業は、ワークステーション上のソーシャル メディア プラットフォームと個人用クラウド ストレージへのユーザー アクセスを制限することで、データ損失防止を実装したいと考えています。これらの目標を達成するには、次のどのタイプのフィルタリングを導入する必要がありますか。
A. DNS
B. ポート
C. MAC
D. コンテンツ
Answer: D (メーッセージを残す**)**

最新問題**: 89**
技術者が理論を確認するために実行する必要があるトラブルシューティング方法論の次のステップはどれですか?
A. 問題が重複しています。
B. 症状を特定します。
C. 情報を収集します。
D. 変更内容を確認します。
Answer: A (メーッセージを残す**)**
トラブルシューティングの方法:
トラブルシューティングには、問題を診断して解決するための体系的なアプローチが含まれます。通常、これには症状の特定、情報の収集、理論の策定とテスト、解決策の実装などの手順が含まれます。
理論の確認:
問題を再現する: 理論を確認するには、技術者は制御された環境で問題を再現する必要があります。これにより、特定された原因が実際に観察された問題につながるかどうかを確認できます。
検証: 問題を再現することで、技術者は問題を直接観察し、仮説を検証し、他の潜在的な原因を排除することができます。
他のステップとの比較:
症状を特定する: 理論を確認するためではなく、問題が何であるかを理解するための最初のステップです。
情報収集: 問題に関するデータと詳細を収集します。通常は理論を立てる前に行われます。
変更の特定: 情報収集フェーズの一部として、問題の原因となった可能性のある最近の変更を確認します。
実装：
テスト環境で同様の機器またはソフトウェアを使用して、問題を再現します。
結果を観察して、それが元の問題と一致するかどうかを確認し、それによって理論を確認します。
参照：
トラブルシューティングの方法論とベスト プラクティスに関する CompTIA Network+ 学習教材。

最新問題**: 90**
コストを削減し、モビリティを向上させるために、最高技術責任者 (CTO) は、組織とその関連会社にクラウド サービスを導入したいと考えています。ユーザーへの影響を軽減するために、CTO は主要なサービスをオンサイト データ センターから実行し、エンタープライズ サービスをクラウドで実行したいと考えています。次の展開モデルのどれが組織にとって最適な選択でしょうか。
A. パブリック
B. ハイブリッド
C. SaaS
D. プライベート

Answer: B (メッセージを残す)
ハイブリッド クラウド導入モデルは、CTO の要件に最適な選択肢です。このモデルでは、組織はオンサイトのデータ センターから主要なサービスを実行しながら、エンタープライズ サービスにクラウドを活用できます。このアプローチは、柔軟性、拡張性、コスト削減を実現すると同時に、重要なサービスをローカルに維持することでユーザーへの影響を最小限に抑えます。ハイブリッド モデルは、プライベート クラウド環境とパブリック クラウド環境の両方を統合し、両方の利点を提供します。
参考: CompTIA Network+ の学習教材とクラウド コンピューティングの原則。

最新問題**: 91**
ネットワーク管理者は各部門にセキュリティ ゾーンを実装しています。このタスクを実行するために管理者は次のどれを使用する必要がありますか?
A. ACL
B. ポートセキュリティ
C. コンテンツフィルタリング
D. NAC
Answer: A (メッセージを残す)
* ACL を理解する:
* アクセス制御リスト (ACL): IP アドレス、プロトコル、またはポートに基づいてパケットをフィルタリングすることにより、ネットワーク トラフィックを制御し、ネットワーク リソースへのアクセスを制限するために使用される一連のルール。
* セキュリティゾーンの実装:
* ゾーンの定義: ACL を使用すると、さまざまな部門に特定のルールを適用してセキュリティ ゾーンを作成し、これらのゾーン間で許可されたトラフィックのみが許可されるようにすることができます。
* トラフィックの制御: ACL はネットワーク境界で受信トラフィックと送信トラフィックを制御し、セキュリティ ポリシーを適用して不正アクセスを防止します。
* 他のオプションとの比較:
* ポート セキュリティ: スイッチ ポートに接続できるデバイスの数を制限し、MAC アドレス フラッディング攻撃を防止しますが、セキュリティ ゾーンの定義には使用されません。
* コンテンツ フィルタリング: 事前定義されたポリシーに基づいて特定のコンテンツへのアクセスをブロックまたは許可します。通常は、ネットワーク セグメンテーションではなく Web フィルタリングに使用されます。
* NAC (ネットワーク アクセス制御): デバイスのセキュリティ状態に基づいてネットワークへのアクセスを制御しますが、セキュリティ ゾーンは定義しません。
* 実装手順:
* 各部門の要件に基づいて ACL ルールを定義します。
* これらのルールを適切なネットワーク インターフェイスまたはファイアウォール ポリシーに適用して、ネットワークをセキュリティ ゾーンに分割します。
参考文献:
* ネットワーク セキュリティとアクセス制御方法に関する CompTIA Network+ 学習教材。

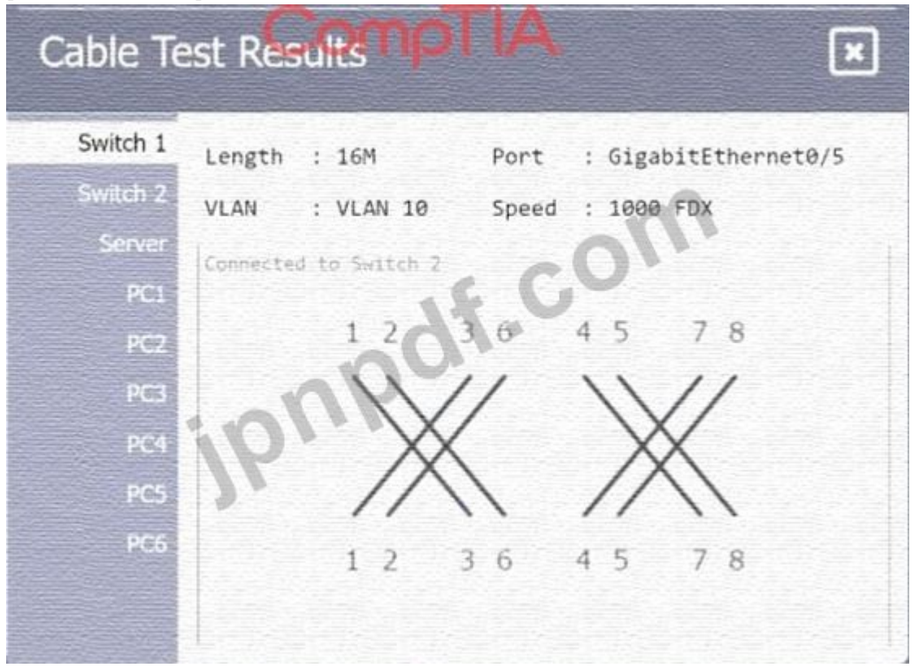
最新問題**: 92**
保険仲介業者が VPN の使用を強制する理由として最も可能性が高いのは次のどれですか?
A. 転送中の機密データを暗号化する
B. エンドポイントを保護する

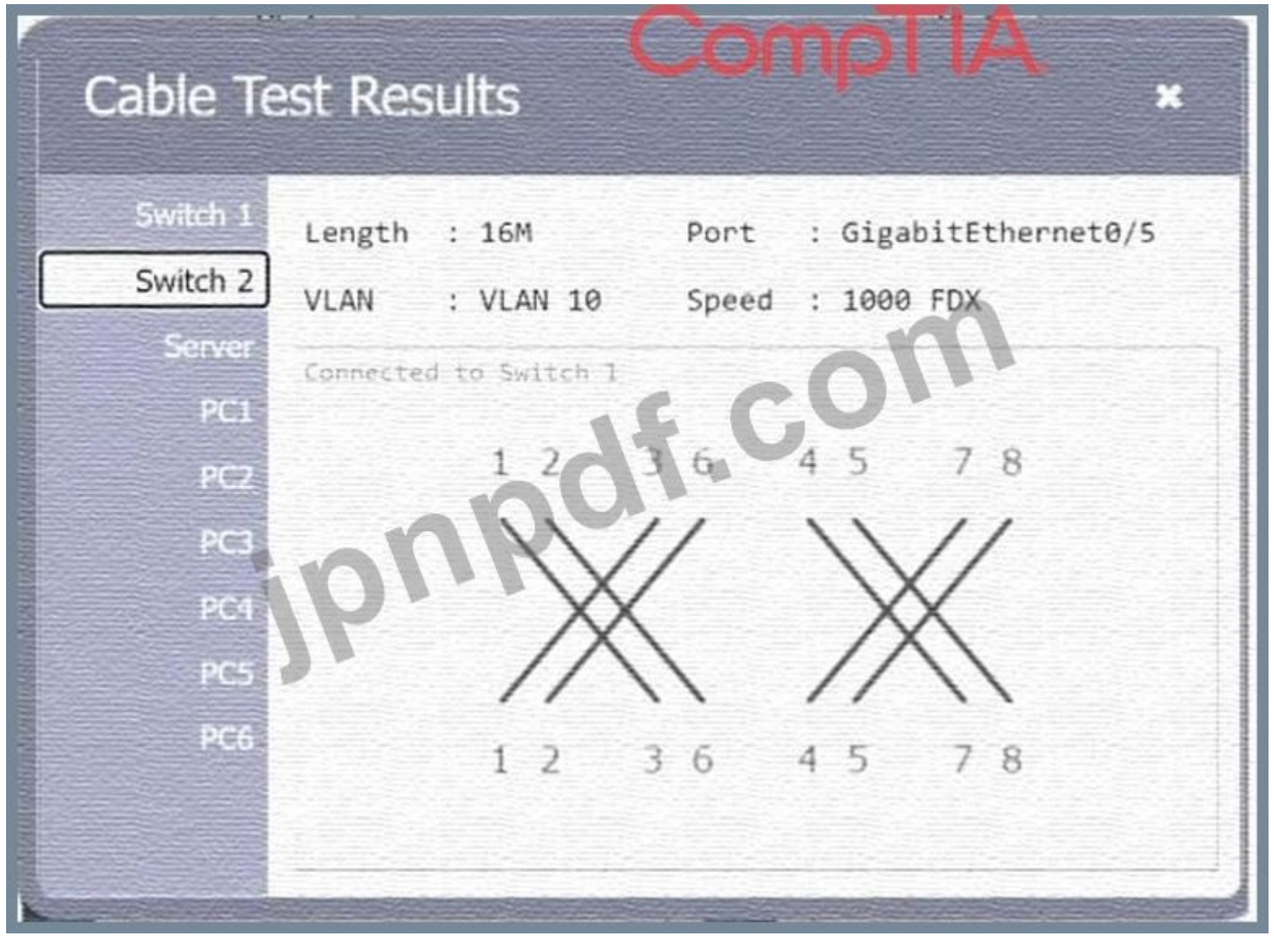
C. 契約上の合意を維持するため
D. データ保持要件に準拠するため
Answer: A (メッセージを残す**)**
保険仲介業者が VPN の使用を強制する最も可能性の高い理由は、転送中の機密データを暗号化することです。
VPN (仮想プライベート ネットワーク) は、ユーザーのデバイスと企業ネットワークの間に安全なトンネルを作成し、データが暗号化され、傍受から保護されることを保証します。
* 暗号化: VPN はデータを暗号化し、不正アクセスを防止し、パブリック ネットワークやセキュリティ保護されていないネットワークを介した送信中にデータのプライバシーを確保します。
* データ保護: 保険仲介業など、機密情報を扱う業界にとって、顧客データを保護し、規制要件に準拠するために不可欠です。
* セキュリティ: 従業員に安全なリモート アクセスを提供することで、ネットワーク全体のセキュリティを強化します。
ネットワーク参照:
* CompTIA Network+ N10-007 公式認定ガイド: 転送中のデータのセキュリティ保護における VPN の役割について説明します。
* Cisco Networking Academy: VPN テクノロジーとデータ セキュリティにおけるその重要性に関するトレーニングを提供します。
* Network+ 認定オールインワン試験ガイド: VPN の使用方法と機密情報を保護する上での利点について説明します。

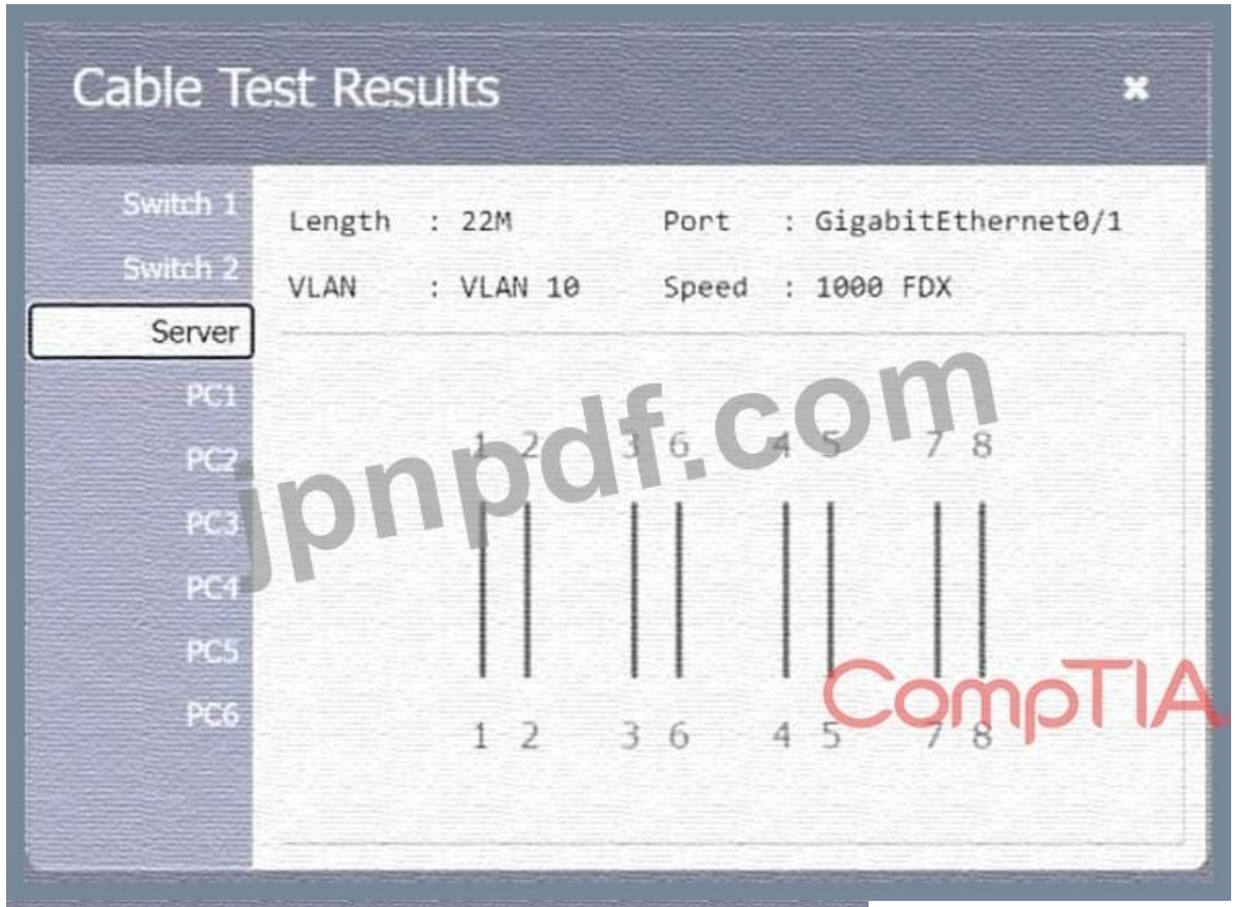
最新問題**: 93**
次のファイバー コネクタ タイプのうち、ネットワーク インターフェイス カードで使用される可能性が最も高いのはどれですか。
A. LC
B. SC
C. ST
D. MPO
Answer: A (メッセージを残す**)**
* ファイバーコネクタタイプの定義:
* LC (Lucent コネクタ): プッシュプル ラッチ機構を備えた小型フォームファクタの光ファイバー コネクタ。高密度アプリケーションでよく使用されます。
* SC (加入者コネクタまたは標準コネクタ): プッシュプルラッチ機構を備えた大型フォームファクタコネクタ。データ通信や電気通信アプリケーションでよく使用されます。
* ST (ストレート チップ): バヨネット スタイルのコネクタ。通常はマルチモード光ファイバー ネットワークで使用されます。
* MPO (マルチファイバー プッシュオン): 高密度ケーブル環境で使用される、複数のファイバー (通常は 12 または 24 ファイバー) をサポートするように設計されたコネクタ。
* 一般的な使用法:
* LC コネクタ: LC コネクタはサイズが小さいため、ネットワーク インターフェイス カード (NIC) やデータ センターなどの高密度環境で広く使用されています。SC コネクタや ST コネクタに比べて、より狭いスペースでより多くの接続が可能になります。
* SCおよびSTコネクタ :これらはより大きく、パッチパネルや古い
* ファイバーの設置に適していますが、高密度アプリケーションには適していません。
* MPO コネクタ: 主にデータ センターや高密度アプリケーションのトランク ケーブルに使用されますが、個々のネットワーク インターフェイス カードでは通常使用されません。
* 選考基準:
* LC コネクタは、小型フォームファクタと高密度機能を備えているため、スペースと接続密度が重要な考慮事項となるネットワーク インターフェイス カードに最適です。
参考文献:
* 光ファイバーとコネクタの種類に関する CompTIA Network+ 学習教材。

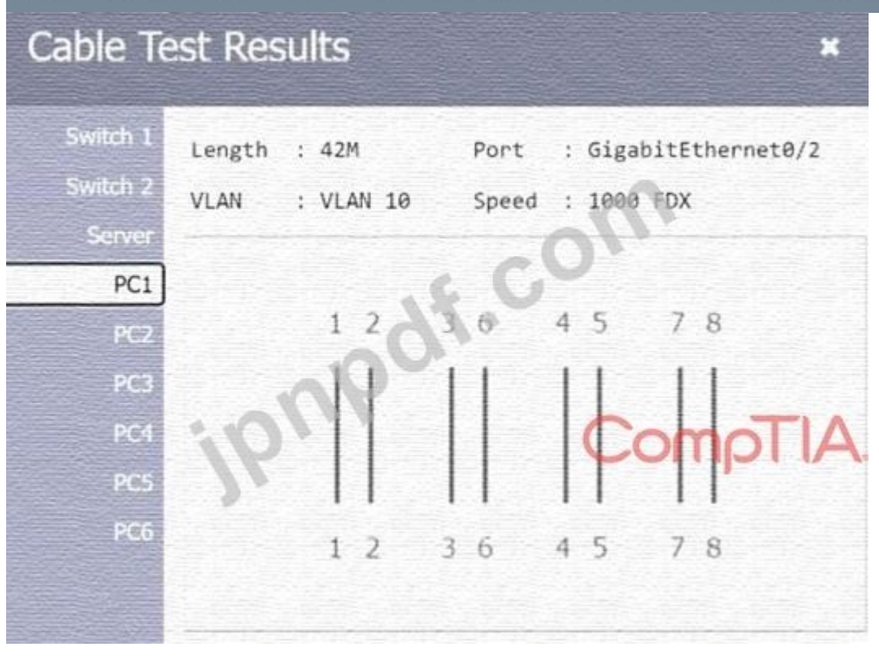
最新問題**: 94**
ネットワーク技術者は、顧客の SOHO ネットワークに関するいくつかの問題を解決する必要があります。顧客は、一部の PC がネットワークに接続されていないが、他の PC は正常に動作しているようだと報告しています。
説明書

すべてのネットワーク コンポーネントのトラブルシューティングを行います。
まずケーブル テストの結果を確認し、適切な PC、サーバー、およびレイヤー 2 スイッチをクリックして診断します。
問題のあるコンポーネントを特定し、それぞれの問題を修正するための解決策を提案します。
いつでも持ち帰りたい場合は
シミュレーションの初期状態を教えてください
[すべてリセット]ボタンをクリックします。







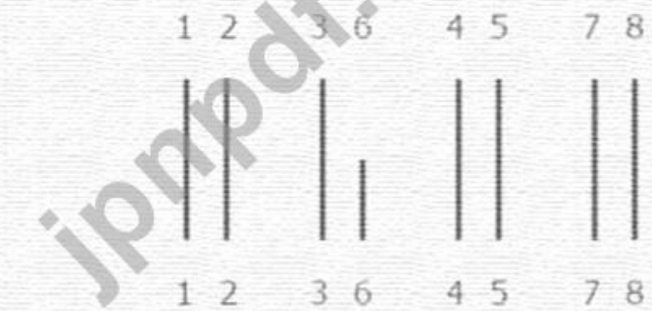


Cable Test Results

Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6

Length : 12M Port : GigabitEthernet0/1

VLAN : VLAN 10 Speed : 1000 FDX

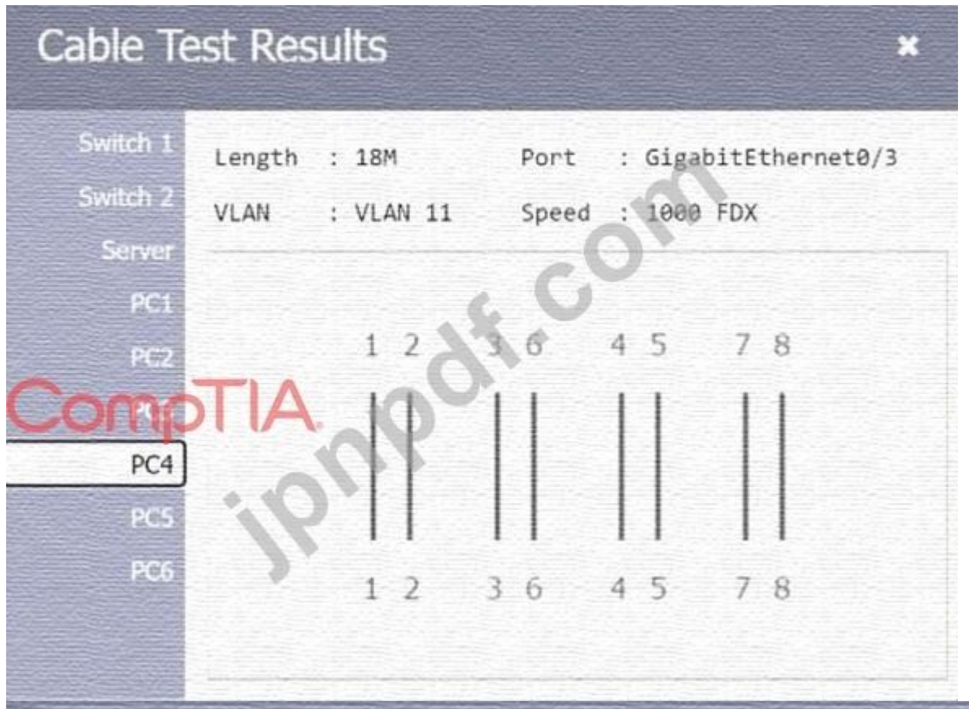


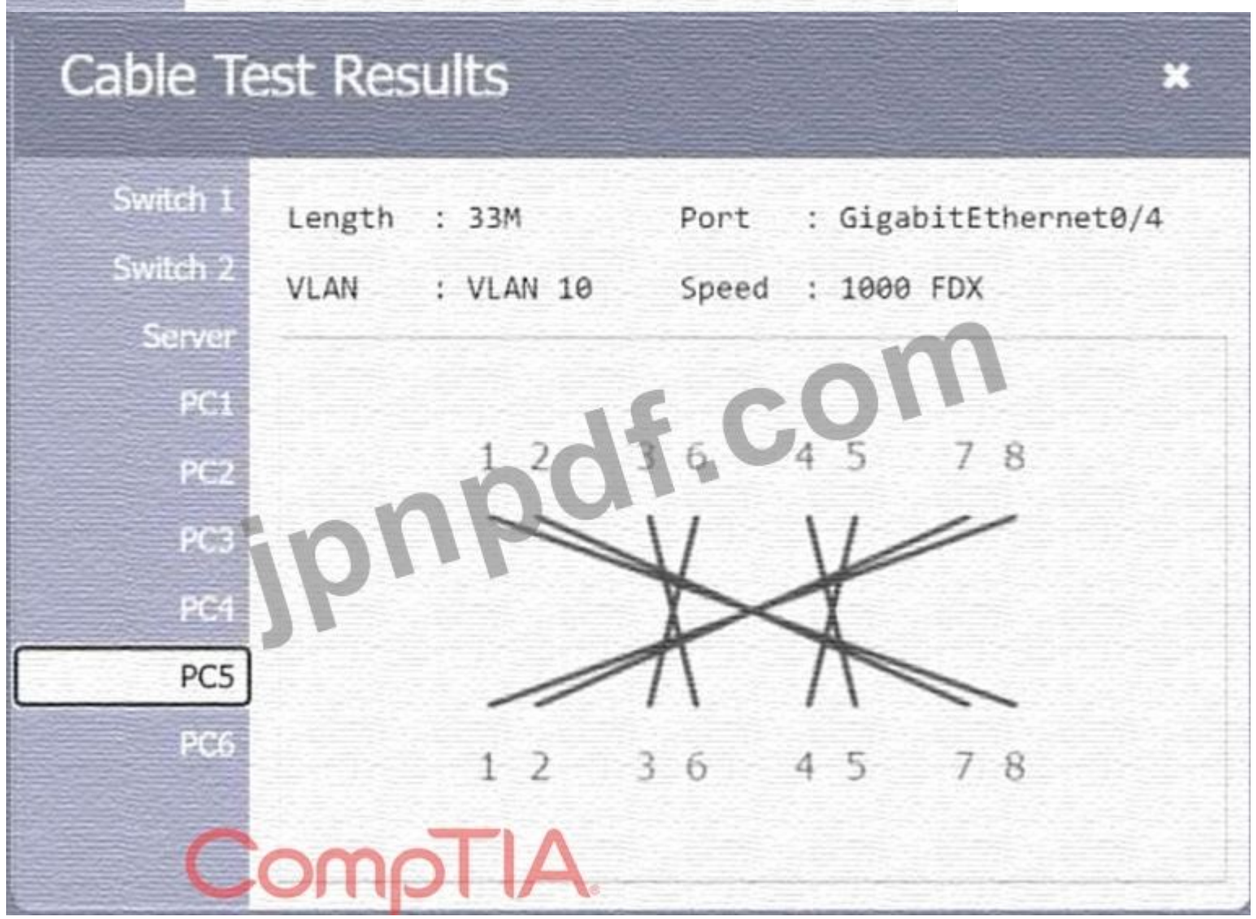
Cable Test Results

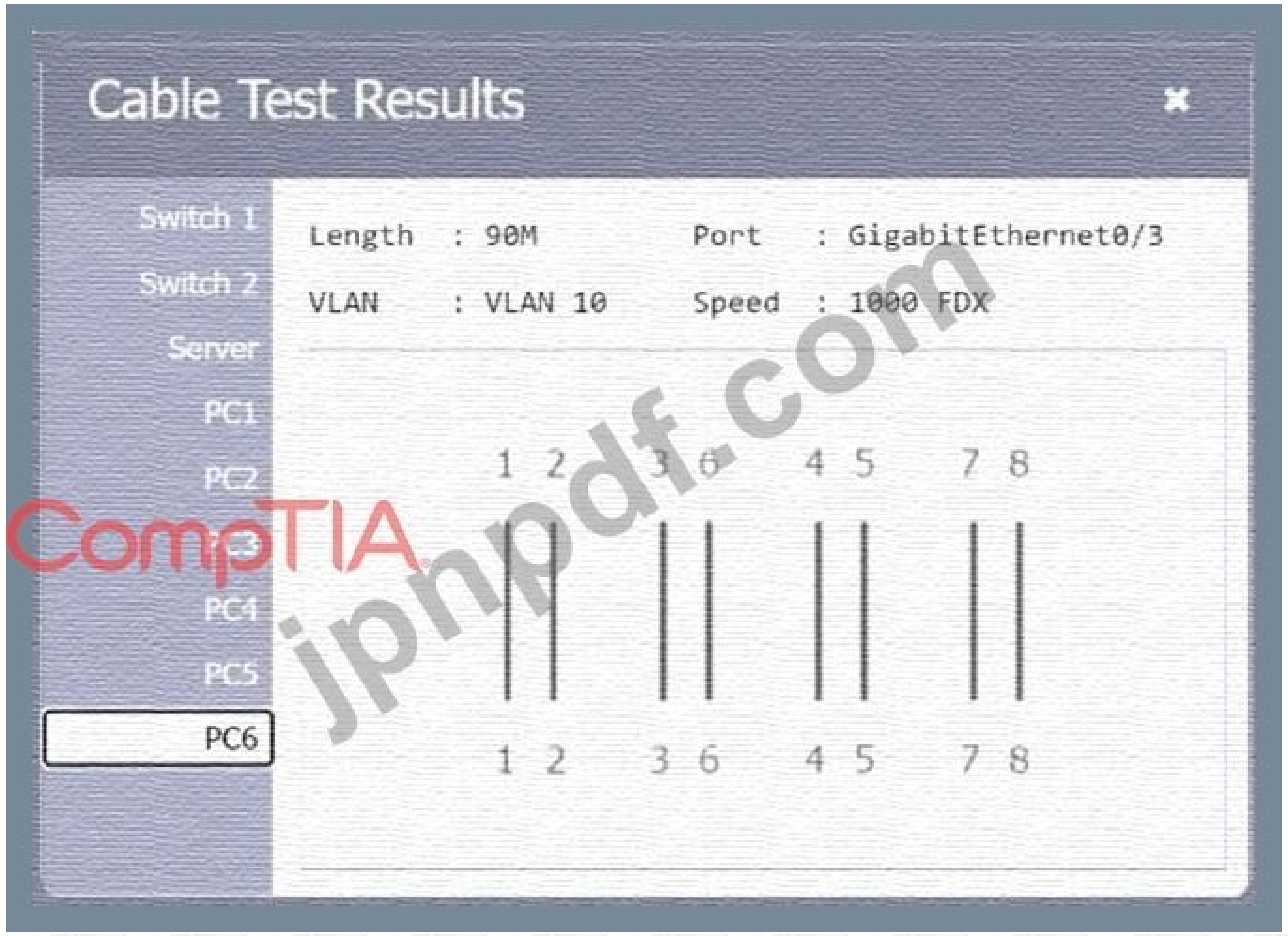
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6

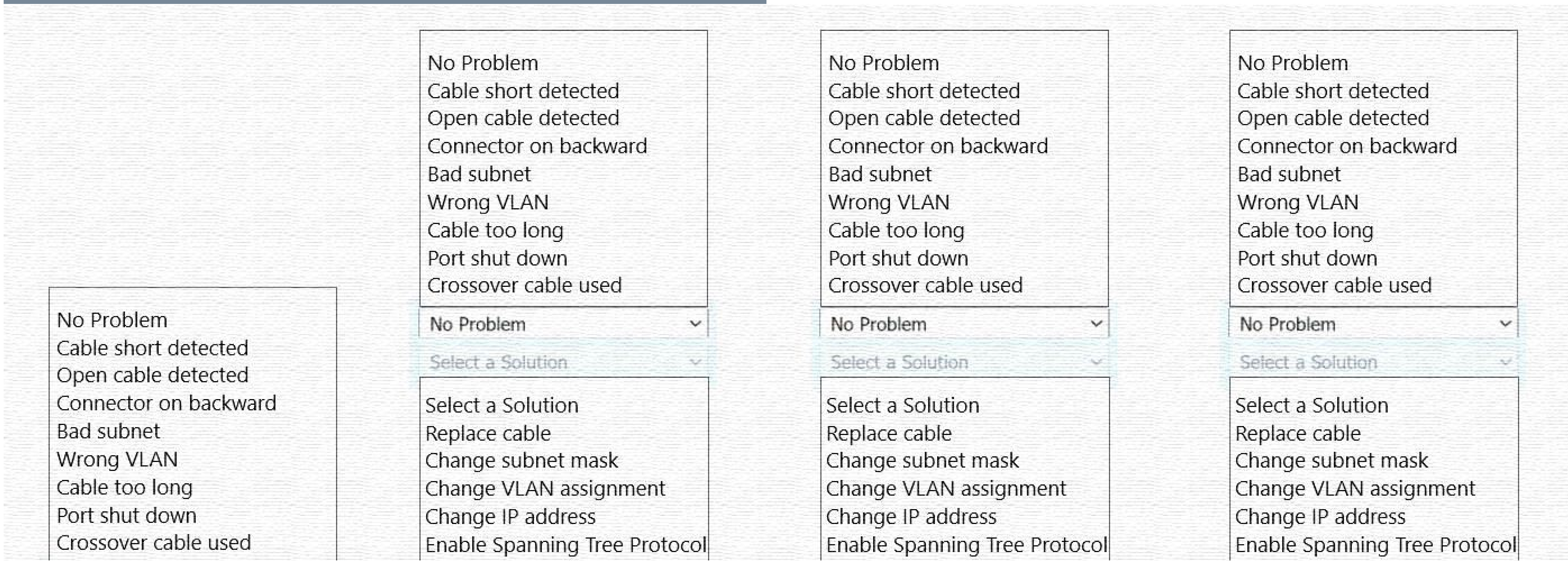
Length : 20M Port : GigabitEthernet0/2

VLAN : VLAN 10 Speed : 1000 FDX









No Problem

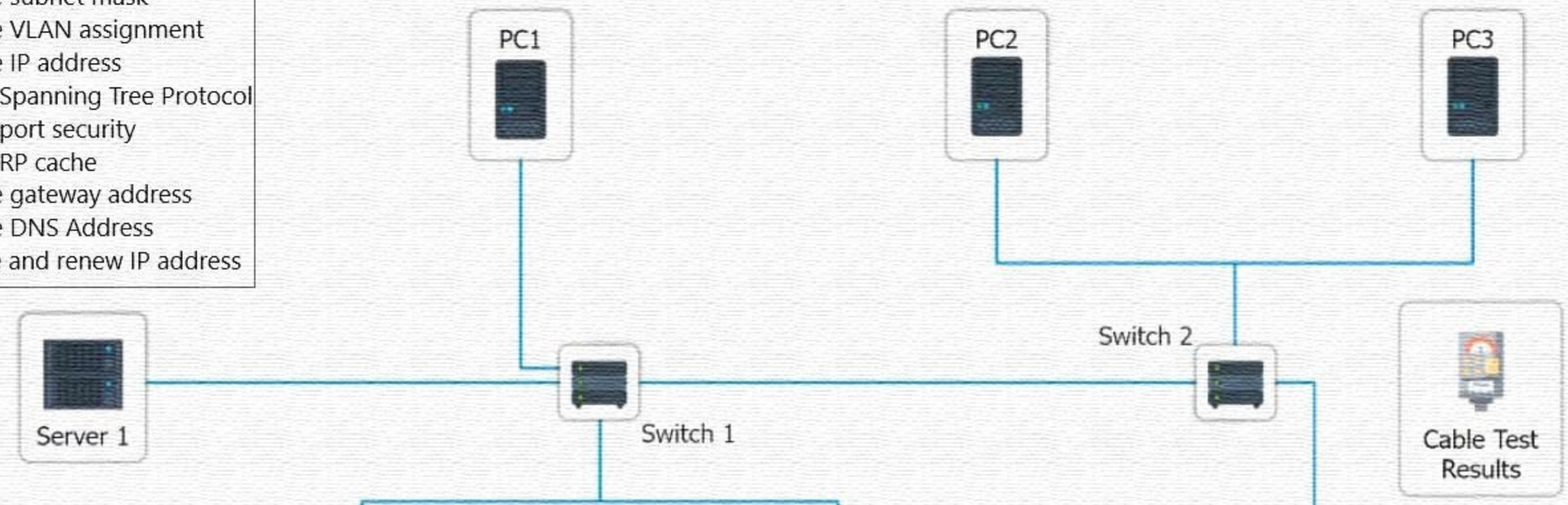
Select a Solution

Select a Solution
Replace cable
Change subnet mask
Change VLAN assignment
Change IP address
Enable Spanning Tree Protocol
Enable port security
Flush ARP cache
Change gateway address
Change DNS Address
Release and renew IP address

Enable port security
Flush ARP cache
Change gateway address
Change DNS Address
Release and renew IP address

Enable port security
Flush ARP cache
Change gateway address
Change DNS Address
Release and renew IP address

Enable port security
Flush ARP cache
Change gateway address
Change DNS Address
Release and renew IP address



No Problem
Cable short detected
Open cable detected
Connector on backward
Bad subnet
Wrong VLAN
Cable too long
Port shut down
Crossover cable used

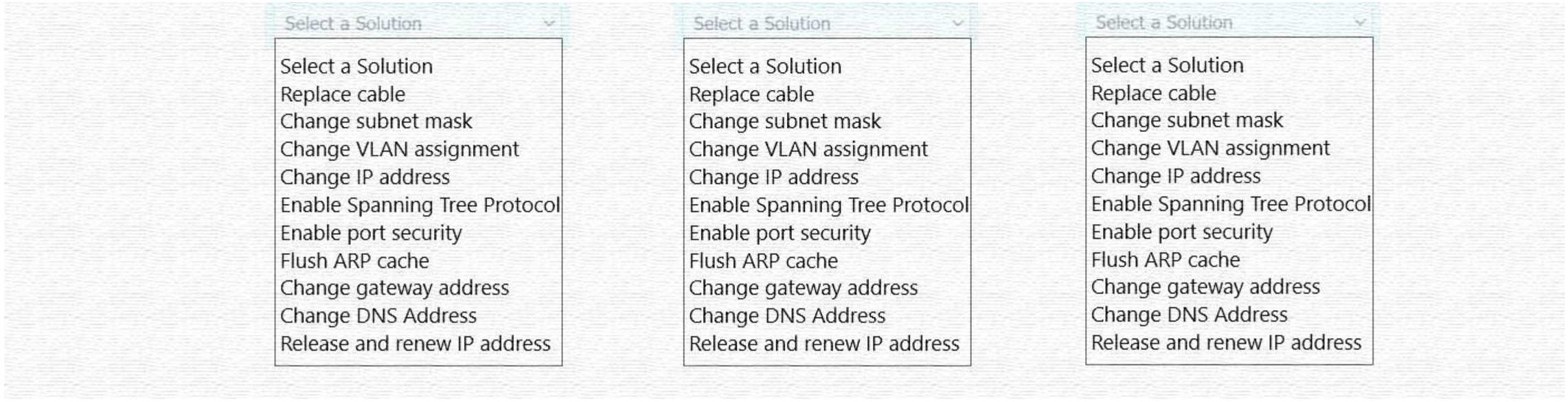
No Problem

No Problem
Cable short detected
Open cable detected
Connector on backward
Bad subnet
Wrong VLAN
Cable too long
Port shut down
Crossover cable used

No Problem

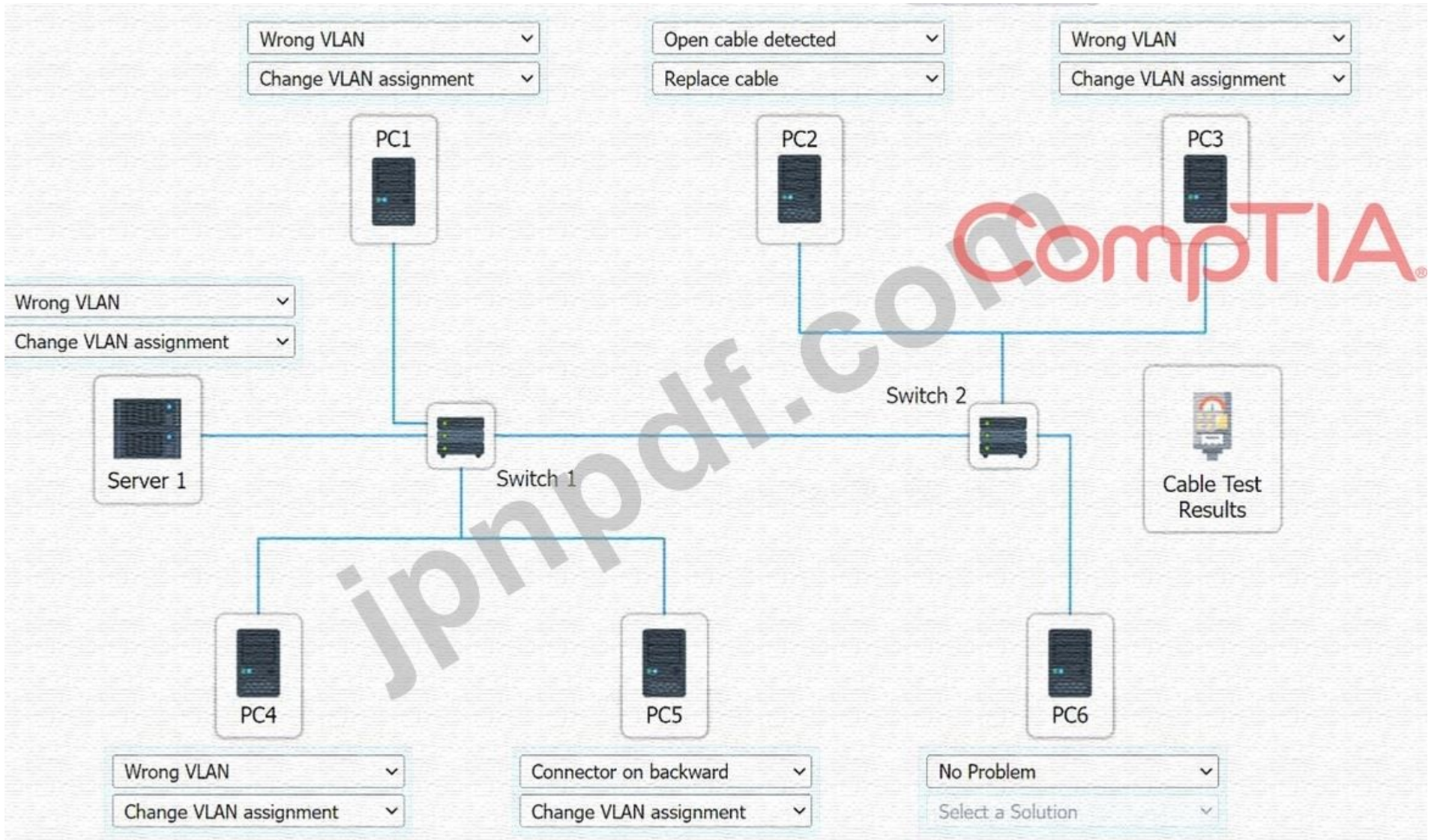
No Problem
Cable short detected
Open cable detected
Connector on backward
Bad subnet
Wrong VLAN
Cable too long
Port shut down
Crossover cable used

No Problem

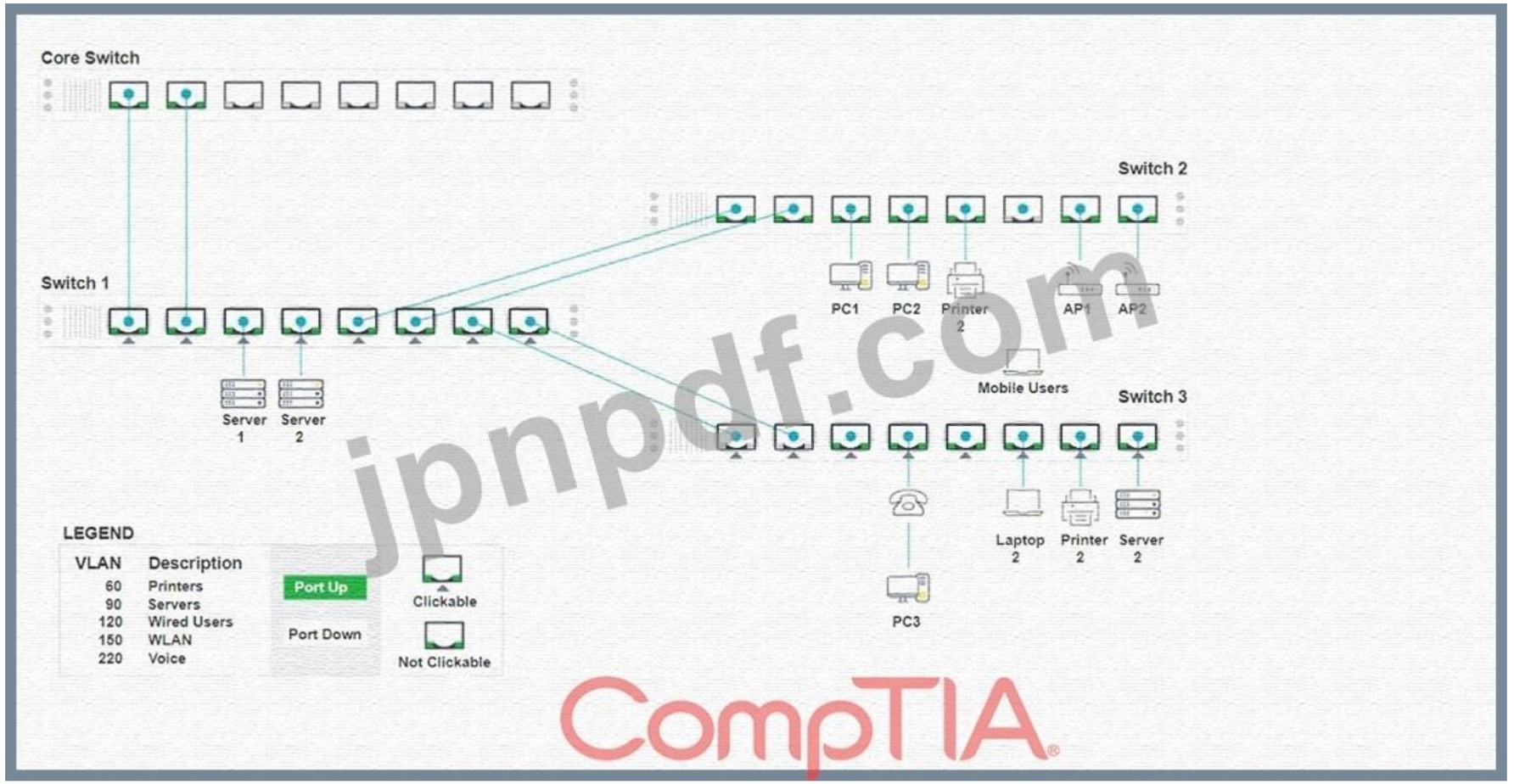


Answer:

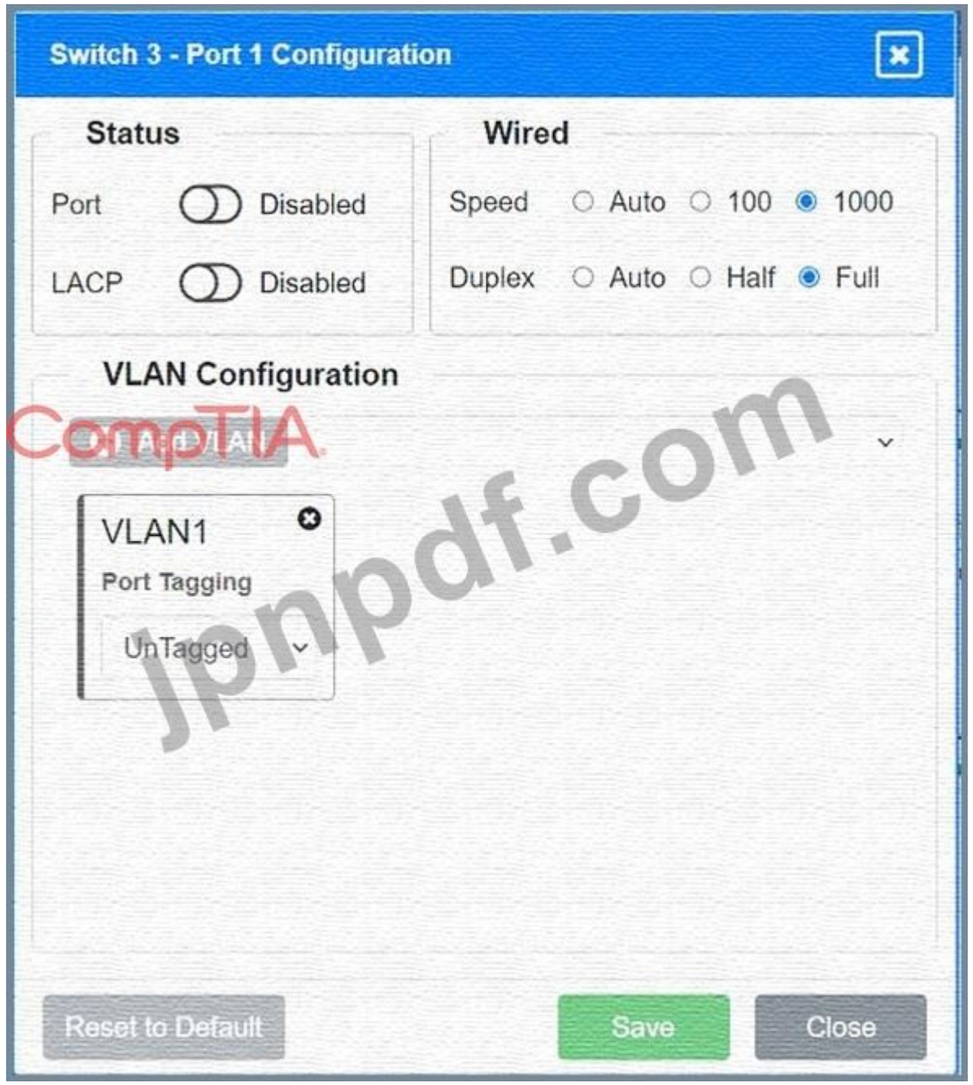
答えと解決策は以下をご覧ください:

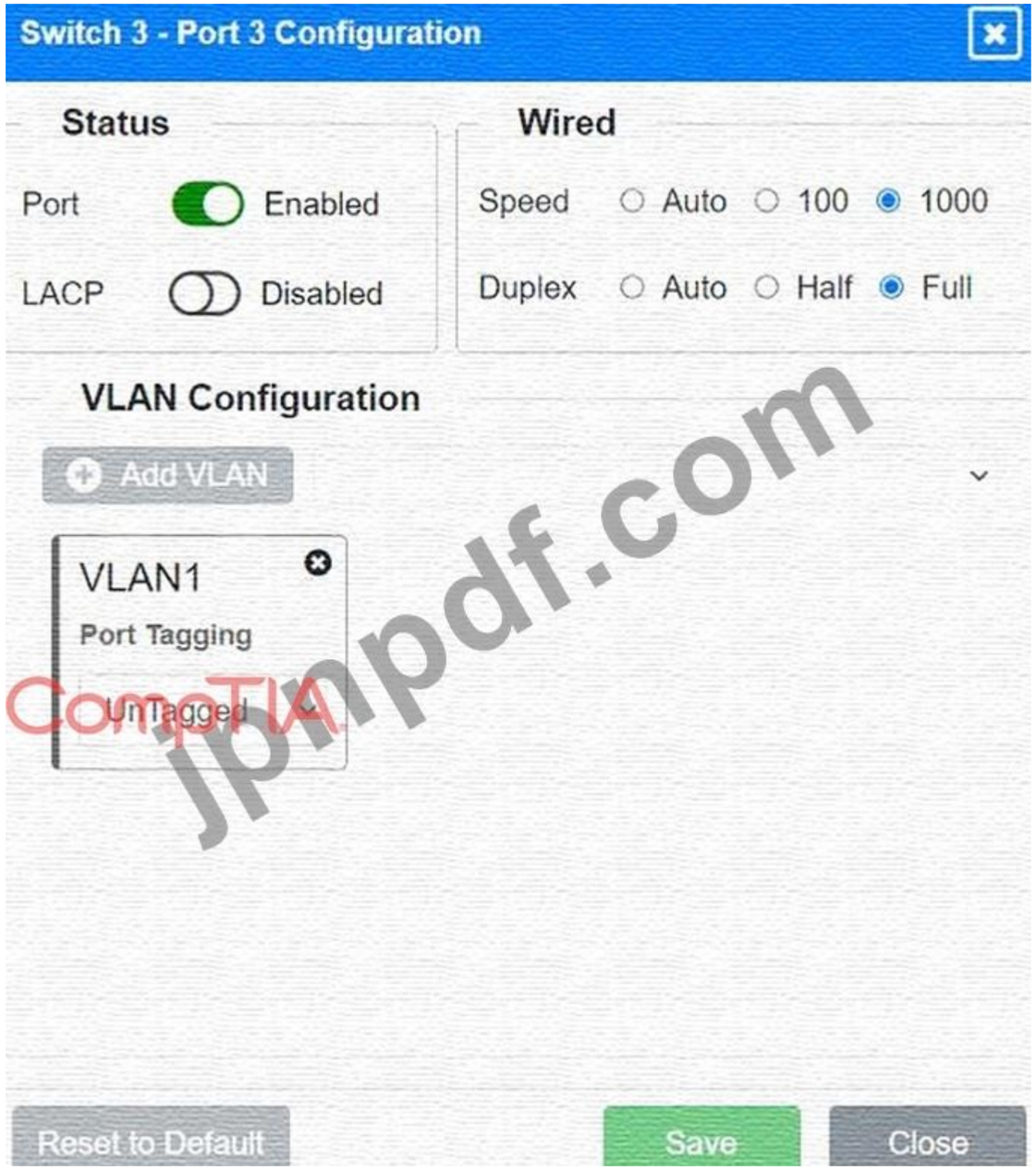


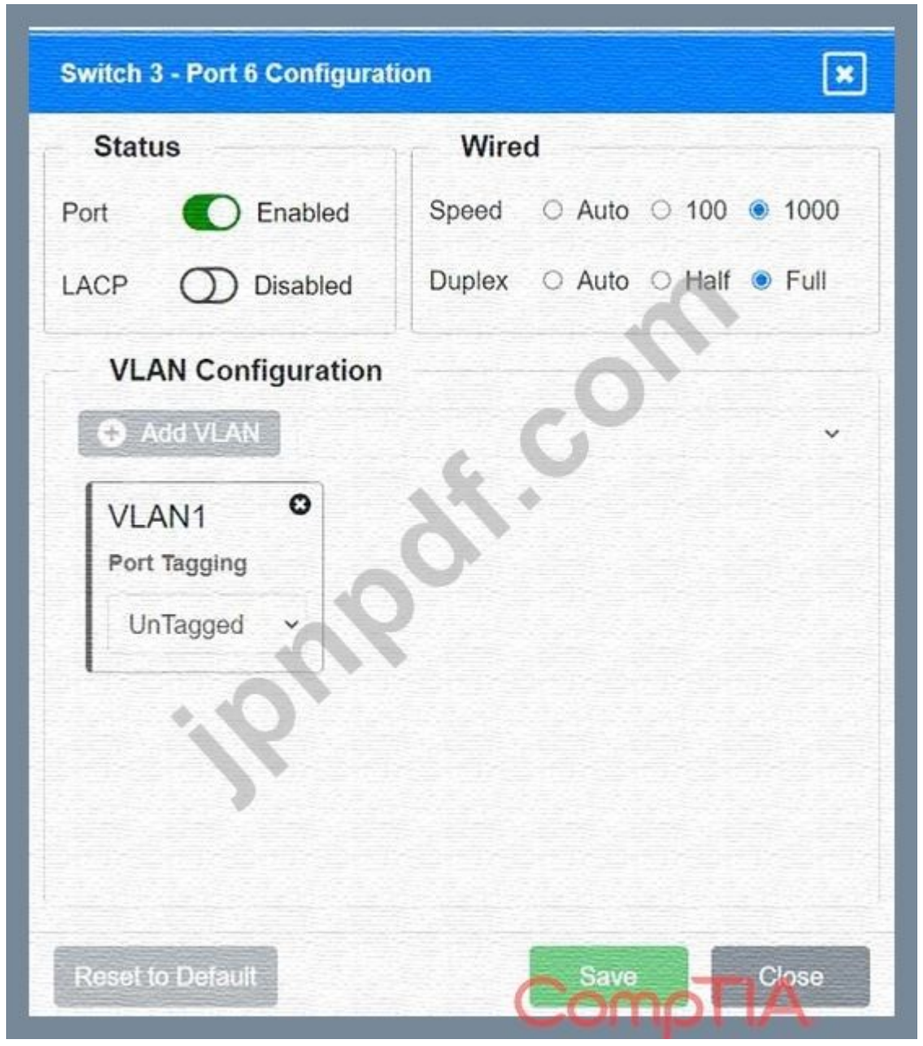
最新問題: **95**
ネットワーク技術者がアクセス レイヤー スイッチを交換し、接続されたデバイスが正しいネットワークに接続できるように再構成する必要があります。
説明書
スイッチ 1 とスイッチ 3 の適切なポートをクリックして、正しい設定を確認または再構成します。
各デバイスが特定のデバイスのみにアクセスできるように
正しく関連付けられたネットワーク。
未使用のスイッチポートをすべて無効にします。
フォールトトレラント接続が必要
スイッチ間。
必要な変更のみ行う
上記の要件を完了してください。

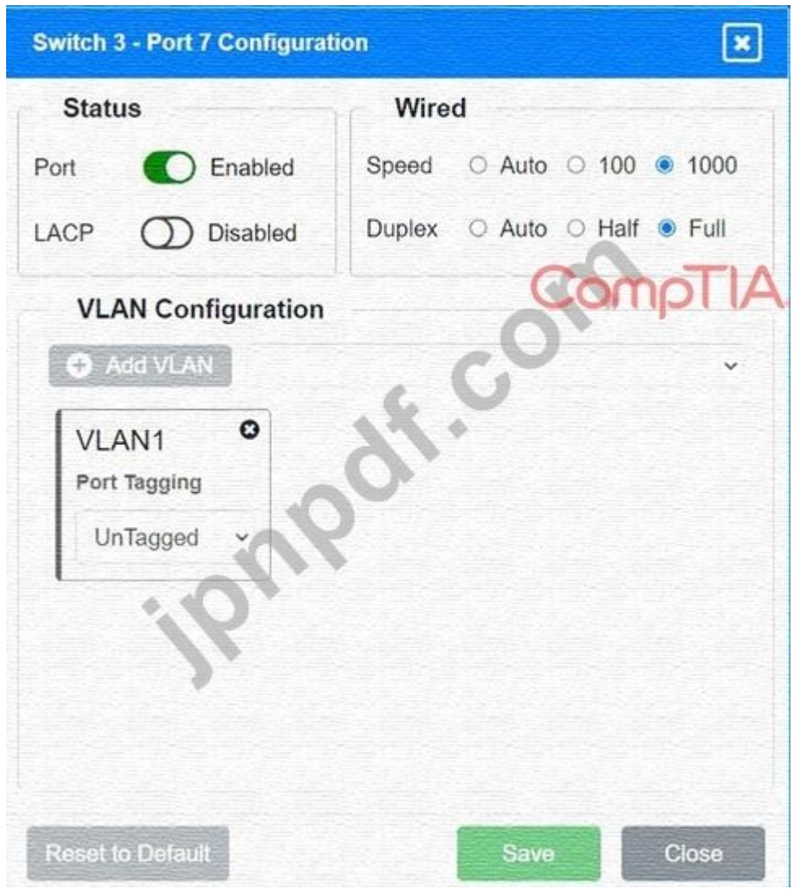

Core Switch
Switch 1
Switch 2
Switch 3
PC1
PC2
Printer 2
AP1
AP2
Mobile Users
Server 1
Server 2
Laptop 2
Printer 2
Server 2
PC3
LEGEND
VLAN Description
60 Printers
90 Servers
120 Wired Users
150 WLAN
220 Voice
Port Up
Port Down
Clickable
Not Clickable
CompTIA

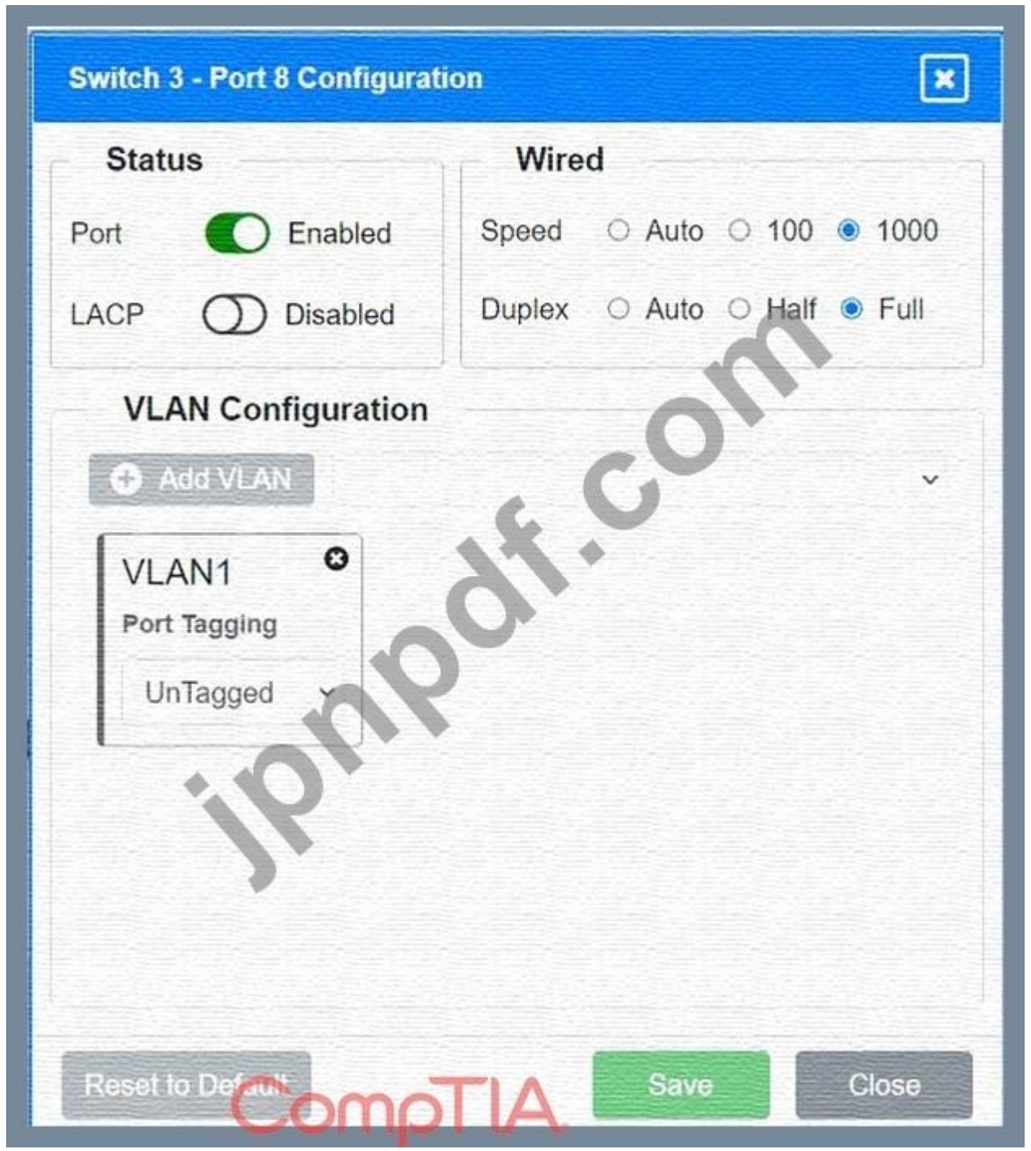

Switch 1 - Port 5 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
CompTIA
Reset to Default
Save
Close

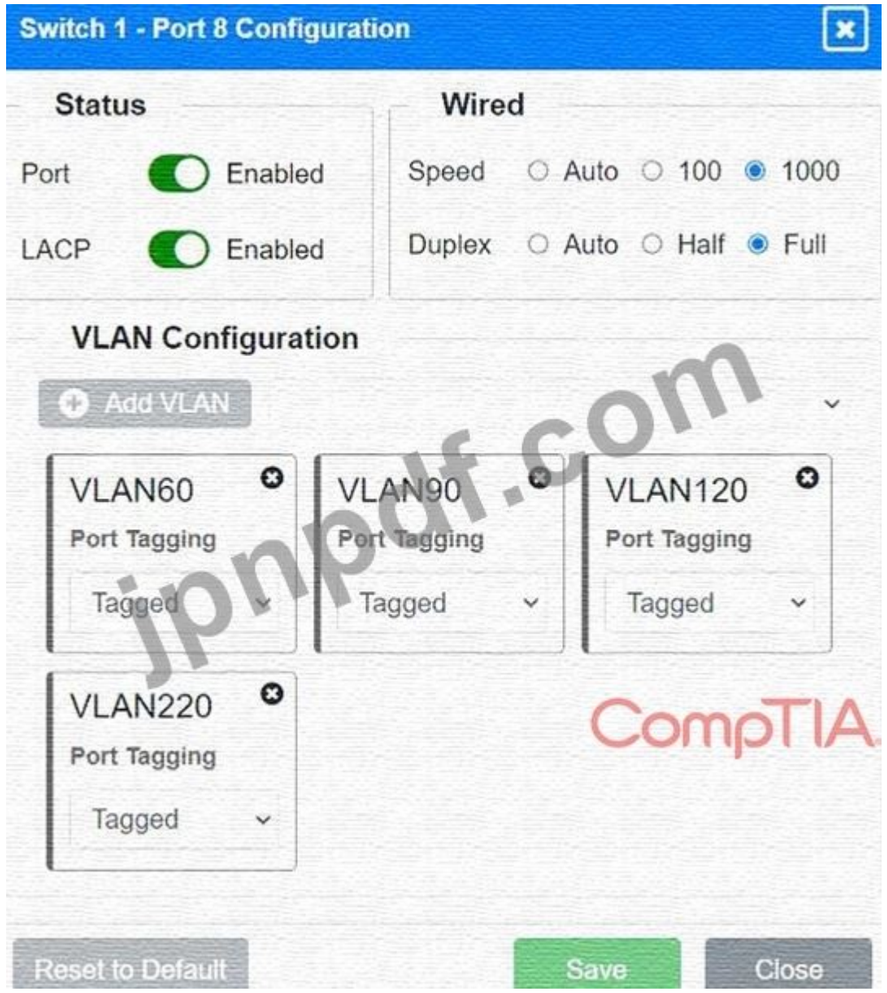












Answer:

下記の説明にある解決策を参照してください。

Explanation:

アクセス レイヤー スイッチを構成するための完全なソリューションを提供するには、次の手順に従います。

* 各デバイスとポートの正しい VLAN を識別します。
* 必要なポートを有効にし、使用しないポートを無効にします。
* スイッチ間のフォールトトレラント接続を構成します。

構成の詳細スイッチ 1 ポート 1 の構成 (コア スイッチへのアップリンク)

* ステータス: 有効
* LACP: 有効
* 速度: 1000
* デュプレックス :フル
* VLAN 構成: VLAN60、VLAN90、VLAN120、VLAN150、VLAN220 のタグ付きポート 2 構成 (コア スイッチへのアップリンク)
* ステータス: 有効
* LACP: 有効

* 速度: 1000
* デュプレックス :フル
* VLAN 構成: VLAN60、VLAN90、VLAN120、VLAN150、VLAN220 のタグ付きポート 3 構成 (サーバー接続)
* ステータス: 有効
* LACP: 無効
* 速度: 1000
* デュプレックス :フル
* VLAN 構成: VLAN90 (サーバー) の場合はタグなし
ポート 4 の構成 (サーバー接続)
* ステータス: 有効
* LACP: 無効
* 速度: 1000
* デュプレックス :フル
* VLAN 構成: VLAN90 (サーバー) の場合はタグなし
ポート 5 の構成 (有線ユーザーと WLAN)
* ステータス: 有効
* LACP: 有効
* 速度: 1000
* デュプレックス :フル
* VLAN設定: VLAN60、VLAN120、VLAN150のタグ付き
ポート 6 の構成 (有線ユーザーと WLAN)
* ステータス: 有効
* LACP: 有効
* 速度: 1000
* デュプレックス :フル
* VLAN設定: VLAN60、VLAN120、VLAN150のタグ付き
ポート 7 の構成 (音声および有線ユーザー)
* ステータス: 有効
* LACP: 有効
* 速度: 1000
* デュプレックス :フル
* VLAN設定: VLAN60、VLAN90、VLAN120、VLAN220のタグ付き
ポート 8 の構成 (音声、プリンター、有線ユーザー)
* ステータス: 有効
* LACP: 有効
* 速度: 1000
* デュプレックス :フル
* VLAN設定: VLAN60、VLAN90、VLAN120、VLAN220のタグ付き
スイッチ 3 ポート 1 構成 (未使用)
* ステータス: 無効
* LACP: 無効

ポート 2 構成 (未使用)
* ステータス: 無効
* LACP: 無効
ポート 3 の構成 (デバイスへの接続)
* ステータス: 有効
* LACP: 無効
* 速度: 1000
* デュプレックス :フル
* VLAN設定: VLAN1はタグなし(デフォルト)
ポート 4 の構成 (デバイスへの接続)
* ステータス: 有効
* LACP: 無効
* 速度: 1000
* デュプレックス :フル
* VLAN設定: VLAN1はタグなし(デフォルト)
ポート 5 の構成 (デバイスへの接続)
* ステータス: 有効
* LACP: 無効
* 速度: 1000
* デュプレックス :フル
* VLAN設定: VLAN1はタグなし(デフォルト)
ポート 6 の構成 (デバイスへの接続)
* ステータス: 有効
* LACP: 無効
* 速度: 1000
* デュプレックス :フル
* VLAN設定: VLAN1はタグなし(デフォルト)
ポート 7 の構成 (デバイスへの接続)
* ステータス: 有効
* LACP: 無効
* 速度: 1000
* デュプレックス :フル
* VLAN設定: VLAN1はタグなし(デフォルト)
* スイッチ 1 のポート 1 と 2 は、必要なすべての VLAN に対して VLAN タグ付けが有効になっているトランク ポートとして設定されています。
* スイッチ 1 のポート 3 と 4 は、タグなし VLAN 90 を使用したサーバー接続用に構成されています。
* スイッチ 1 のポート 5、6、7、8 は、複数の VLAN へのアクセスを必要とするデバイス用に構成されています。
* スイッチ 3 の未使用ポートは無効になります。
* スイッチ 3 のポート 3、4、5、6、および 7 は、デフォルトの VLAN 1 に対して有効になっています。
* コア スイッチ ポートは、スイッチ 1 へのアップリンクに応じて必要に応じて構成する必要があります。
* スイッチ間のトランク ポートの冗長性を確保するために、LACP が有効になっていることを確認します。
構成の概要すべてのスイッチとポートが要件に従って構成されていることを確認します。これらの構成に従うことで、各デバイスは正しく関連付けられたネットワークのみにアクセスし、未使用のス

イッチ ポートは無効になり、スイッチ間にフォールト トレラント接続が確立されます。